ArcSight Web™ User's Guide

ArcSight Express v3.0
Featuring ESM with CORR-Engine Storage

August 2011

ArcSight™
An HP Company

ArcSight Web™ User's Guide ArcSight Express™ v3.0

Revision History

Date	Product Version	Description
07/27/2011	ArcSight Express v3.0	For ArcSight Web embedded in the Management Console

Document template version: 1.0.2.9

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal/
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1

Welcome to ArcSight Web

ArcSight Web is the web interface to monitoring and reporting features of ArcSight ESM for operators and analysts engaged in network perimeter and security monitoring. ArcSight Web for ArcSight Express v3.0 is presented as part of the Management Console. For more about the Management Console, see the *Management Console User's Guide*.

ArcSight Web offers opportunities for custom branding and styling.

To get started using the ArcSight Web interface, see the introduction to "ArcSight Express Content" on page 11 if you have an ArcSight Epxress deployment.

See "Navigating ArcSight Web" on page 7 for a quick tour of all ArcSight Web's features.

Chapter 2

Navigating ArcSight Web

Access the ArcSight Web server through whichever web browser you prefer: Internet Explorer 8.0+ or Firefox 3.6+. The ArcSight Web home URL is `https://hostname:9443/arcsight/app`, where *hostname* is the machine on which the web server is running.

Navigating the Home Page

The ArcSight Web client opens to the Home display. From here you can easily reach everything the client offers.

The Home display's summaries are quick references and links to the most-appropriate or most-interesting security resources in your enterprise. The initial or default information in each group is configured by your ArcSight administrator. In the sections that offer a **Show** menu, you can choose **Start Up View** to see this default or **Personal Folder** to switch to resources selected by or assigned to you.

The information summarized in the Home display is identical to, although possibly a subset of, the same information managed through the ArcSight Console. It is simply presented in a browser-compatible format.

Home

The Home link returns you to the home page from any other view.

Dashboards

The Dashboards section lists a set of data monitor dashboards that expose selected analytical security information about your enterprise. Click a dashboard's name to open it.

Reports

The Reports section lists available reports. Reports are captured views or summaries of data extrapolated from the ArcSight System by means of queries and trends. Reports communicate the state of your enterprise security. Click a report, set the parameters or accept the defaults (HTML or PDF), and click **Run Report**. You have the option of saving the Report results in a variety of file formats to your local system, or just viewing the results in the ArcSight Web window.

Active Channels

Active Channels display the filtered events as they stream through the system. Click a channel to open it as a grid view in which you can inspect individual events. You can pause channels, and sort event columns in the grid.

Cases

The Cases section summarizes currently tracked, event-related security situations by the area they fall into (rows) and the workflow-style stage they have reached (columns). Click a type and stage cell to see more detail.

Recent Notifications

The Recent Notifications section summarizes ArcSight notifications by workflow-style categories. Click a category to see more detail.

Basic Navigation

Use the Dashboards, Reports, Channels, Cases Notifications, and Knowledge Base links at the top of the display to go to those features. A link to **ArcSight Support** is also provided.

Button	Description
	Home
	Dashboards
	Reports
	Channels
	Cases
	Notifications

The top bar also has the client's basic controls.

- Click **Help** to open this Help window. To visit previously viewed Help pages, you can use standard keyboard commands for **Back** and **Next**. For example, on most Web browsers running on Microsoft Windows systems, you can hit the **Backspace** key to show the previously viewed page (move backward in the History) and **Shift + Backspace** to move forward in the History of viewed pages. For more information on using the Help (including how to print topics and get a PDF), see Chapter 3, About the Online Help, on page vii.
- Click **Options** to change your preferences concerning date and time formats, locale settings, active channel setup, and your password.
- Click **Logout** to leave the client and log in again, or browse elsewhere. If you leave the client idle for a period of time you may need to log in again because of an automatic security time-out.
- Click the ArcSight logo in the upper-left corner of the Home display to see version and licensing information.

Chapter 3

ArcSight Express Content

ArcSight Express is an Information and Event Management (SIEM) appliance that provides essential network perimeter and security monitoring tools combined with the Correlation Optimized Retention and Retrieval Engine (CORRE). ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

ArcSight Express content is designed to give you comprehensive operational function out of the box with minimal configuration.

These resources enable you to use the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

ArcSight Express Home Page

The ArcSight Express home page displays a series of basic views designed to give you an overview of activity that concerns you. These views are described below.

Recent Notifications

Recent notifications show the status of notifications generated by correlated events that concern you. To view the details of a notification, click any line item to go to the Notifications page. For more about notifications, see "Handling Notifications" on page 101.

My Cases

My cases show a snapshot of cases assigned to the user who is currently logged in. For details, click the cases icon to go to the Cases page. For more about cases, see "Using Cases" on page 93.

Dashboards

Dashboards show a selection of key dashboards. You can select among these views:

- **Start Up View**: The start-up view provides quick access to the Security Activity Statistics and Current Event Sources dashboards. These dashboards give you a comprehensive general view of the security state of your environment and the sources where the events are generated.
- **Recent Dashboards**: This view shows the last five dashboards you viewed to enable you to easily toggle among several dashboards without having to navigate to them in the Dashboard tab.

Click any of these links to display the dashboard itself.

Active Channels

- **Start Up View**: The start-up view provides a link to the Correlated Alerts channel, which shows all events generated by rules. These events are considered to be events of interest that warrant attention.

- **Personal Folder**: This view contains active channels that you have modified and saved.
- **Recent Channels**: This view shows the last five active channels you viewed to enable you to easily toggle among several active channels without having to navigate to them in the active channels tab.

For more about the home page, see "Navigating ArcSight Web" on page 7.

Getting Started Using ArcSight Express Content

Whatever your role in the security operations center, you can get started right away using the ArcSight Express content.

ArcSight Express Groups

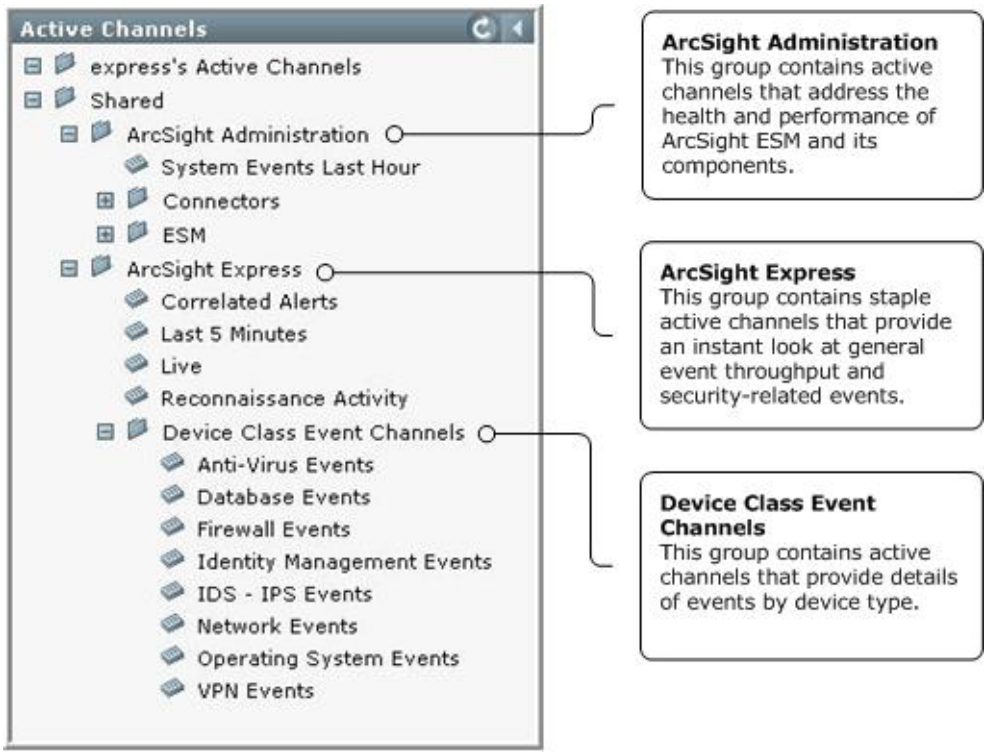
ArcSight Express content is organized into the following device groups relevant to the function the content performs:

Function	Description
Cross-Device	This group contains resources that monitor and report on functions that apply to multiple kinds of devices, such as login attempts, bandwidth usage, and configuration changes.
Anti-Virus	This group contains resources that support monitoring and reporting on anti-virus activity, such as update status, virus activity, and configuration changes.
Case Management	This group contains resources that support monitoring and reporting on activity and notifications involving cases opened in ArcSight as a result of activity that warrants investigation.
Database	This group contains resources that monitor and report on database activity, such as configuration changes, database logins, errors and warnings.
Firewall	This group contains resources that monitor and report on firewall activity, such as network logins and logouts, denied connections, bandwidth usage, and configuration changes.
Identity Management	This group contains resources that monitor and report on user activity, such as logins, user session durations, and configuration changes in order to identify who is doing what activity on the network.
IDS-IPS	This group contains resources that monitor and report on activity involving Intrusion Detection and Prevention Systems, such as signature updates, alerts, and statistics.
Network	This group contains resources that monitor and report on activity involving network infrastructure, including system up/down status, configuration changes, bandwidth usage, and login events.
Operating System	This group contains resources that monitor and report on activity involving operating systems, such as user logins, and user modification events.
VPN	This group contains resources that monitor and report on activity involving VPN connections, including authentication errors, logins, and connection status.
Vulnerabilities	This group contains resources that monitor and report on exposed vulnerabilities by asset.

Monitoring with ArcSight Express Active Channels

The active channels contain three major groups of channels:

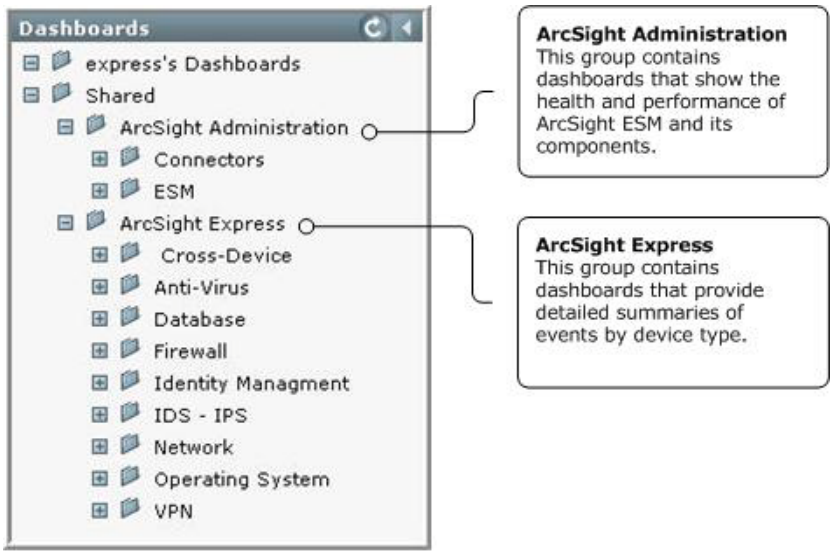
- ArcSight Administration
- ArcSight Express
- Device Class Event Channels



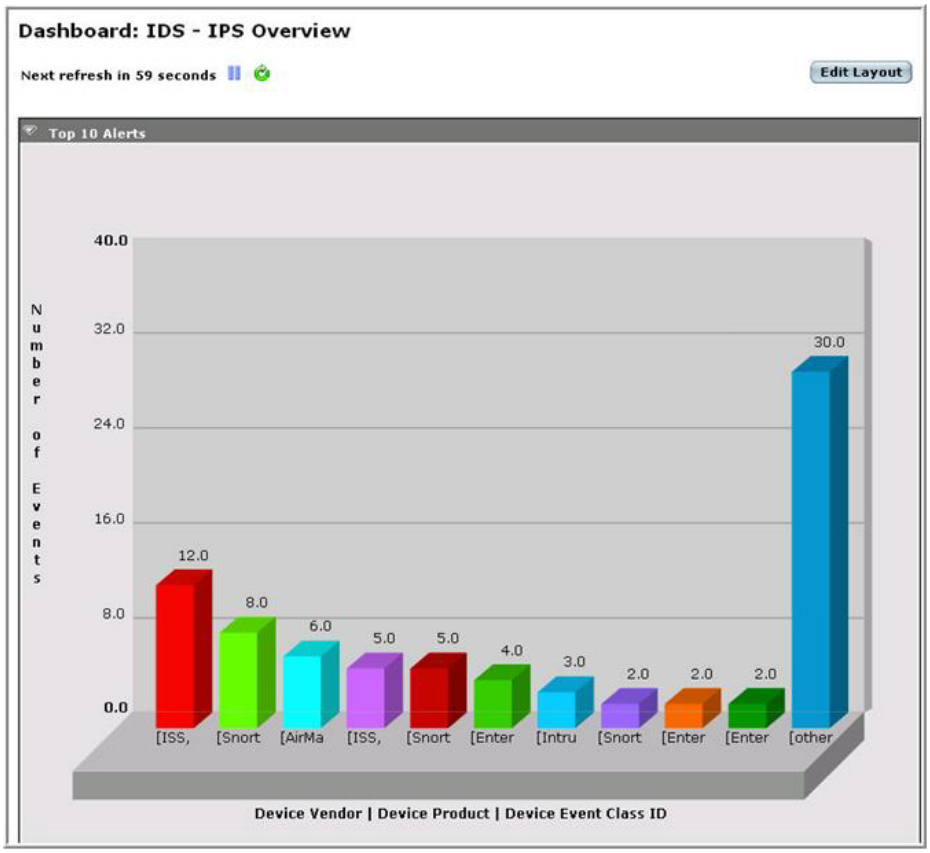
The staple active channels in the ArcSight Express group are a good place to start for monitoring event flows. For instructions about how to use active channels, see "Using Active Channels" on page 17.

Monitoring with ArcSight Express Dashboards

The dashboards contain the ArcSight Administration and ArcSight Express groups. Explore the dashboards to find views you are interested in.



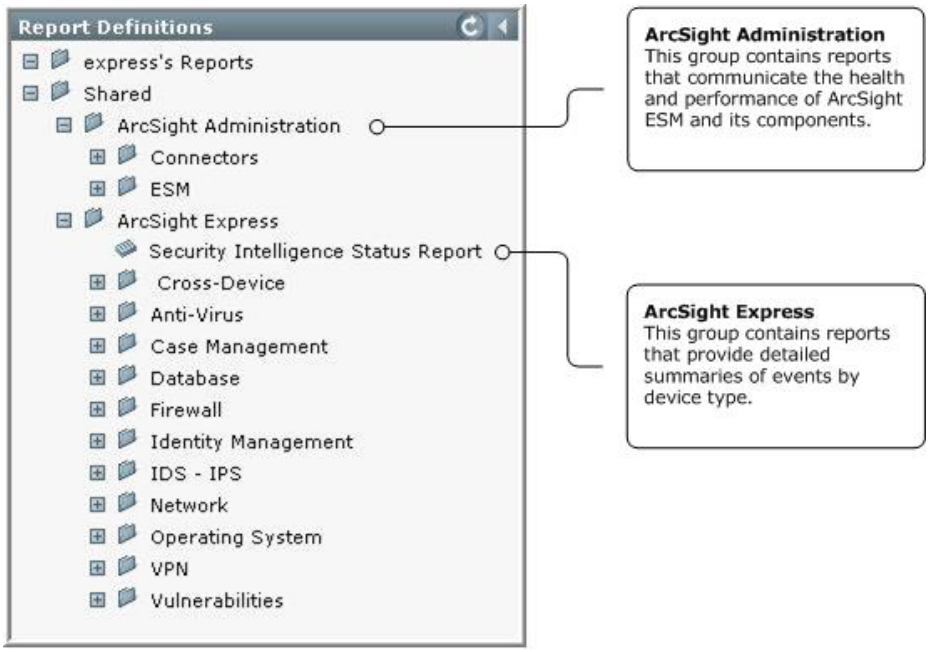
The example below shows the IDS-IPS dashboard, which summarizes the number of events from IDS and IPS systems. Click on any bar to view the details of the events represented in this bar in a channel.



For more about working with dashboards, see “Monitoring Dashboards” on page 109.

Reporting with ArcSight Express Reports

The reports also contain the ArcSight Administration and ArcSight Express groups.



The Security Intelligence Status Report provides a summary of event counts and top events, attacks, targets, ports, and so on, as shown in the example below.

For more about working with reports, see “Using Reports” on page 103.

Chapter 4

Using Active Channels

The event information presented in the ArcSight Web active channel views is the same data presented in the Console. The web client makes channels accessible from anywhere on your enterprise network, or even outside a firewall.

Using active channels includes opening them, controlling their views, and drilling down into the individual events that channels collect.

Opening Active Channels

To open an active channel, click its name in the Active Channels section of the Home display, or click the Channels icon in the toolbar and choose a channel in the Active Channels resource tree. Channels you click in the Home display open directly, but channels you choose in the resource tree offer a setup page before opening.

Use the Open Active Channel setup display to adjust the timing, filter, and column-set parameters of the channel, if necessary. This display appears unless you have turned channel setup off (bypass channel setup) in the Channels panel of the Options display.

There is also an option to hide (collapse) the channel tree on the left panel when a channel is already running. By default, this tree remains in view. Click the Show () or Hide () buttons at the top of the left panel to show or hide the folder tree.

Active Channel Parameters

Option	Description
Channel	Read-only field that shows the channel name.
Start Time	The relative or absolute time reference that begins the period in which to actively track the events in the channel. Edit the time expression or clear the **Date expression** check box to use an absolute date and time.
End Time	The relative or absolute time reference that ends the period in which to actively track the events in the channel. Edit the time expression or clear the **Date expression** check box to use an absolute date and time.

Option	Description
Evaluate parameters continuously	Choose whether the channel will show events that are qualified by Start and End times that are re-evaluated constantly while it is running (selected), or show only the events that qualify when the channel is first run (cleared).
Use as Timestamp	Choose the event-timing phase that best supports your analysis. **End Time** represents the time the event ended, as reported by the device. **Manager Receipt Time** is the event's recorded arrival time at the ArcSight Manager.
Field Set	The Field Set you choose here determines which columns will show up in the active channel display. By default, a standard list of columns is shown in the channel. Choose an existing field set to control the selection and order of the columns in the grid or choose **More Choices** or click the plus sign (+) to open the Field Sets resource tree. The **None** option clears a field set and restores the channel to its original definition. Global variables make it possible to define a variable that derives particular values from existing data, then re-use it in multiple places wherever conditions can be expressed, and wherever fields can be selected. For more informatin about global variables, see "Global Variables" on page 441, in the *ESM Console User Guide*.the Domain Field Sets topic
Filter Override	You can use the Filter Override to narrow the event flow in the channel to only those events that satisfy conditions you specify here. You have these options for Filter Override: • Simply choose an existing filter. You can choose a recently used filter from the drop-down menu, or navigate to other filters by clicking **More Choices** or clicking the plus sign (+) to override the default channel filter. (The **None** option clears a filter choices and restores the channel to its original definition.) Or • Explicitly specify new filter conditions for the channel by using event attributes (field groups and fields) or an existing filter (MatchesFilter) as part of a condition. the Domain Field Sets topicYou can review the conditions of the filter in the active channel header (see "Using Active Channel Headers" on page 19).

Viewing Active Channels

This topic explains how to understand, change, and drill into the grid views of active channels.

Using Active Channel Headers

Using active channels begins with reading and understanding their headers. Headers display the following information:

Feature	Usage
Name and Total	The top line of the header shows the channel's name and the percentage of qualifying events that are currently loaded in the view.
Time Span	The Start Time and End Time show the chronological range of the channel.
Evaluation	This flag indicates whether the channel is set to evaluate events continuously as they are received, or only once when the channel opens. Click **Modify** to change this parameter.
Filter	This text describes the filter that limits what the channel shows.
Priority Totals	On the right side of the header is a column of event-priority category totals. The figures are the number of events in those categories.
Channel State	The channel state box contains a play and pause button and a refresh progress bar. This display indicates whether the channel is running or paused, and if it is running, the progress of the next refresh cycle.
Radar Display	The Radar display in active channel headers indicates the activity taking place in the entire channel (not just the current page). Its graphics represent units of time horizontally, and numbers of events in vertical bars segmented by Priority attribute-value counts. The time and quantity scales in the graphic automatically adjust to accommodate the scope of the channel. The broader the scope, the smaller the graphical units become. To focus the grid on the event of one period, click that bar in the display. To restore the display, click **Clear** at the right end of the bar. Your sorting choices in the grid affect the arrangement of the activity units in the Radar.
Time Range	The Displaying bar below the Radar display and above the grid header shows the time range of the events selected in the Radar display and reflected in the grid. If nothing is selected, the time range shows **All**.

Using Active Channel Grids

Event grids display the individual events that active channels capture.

To page through a grid

Click the navigation buttons on the right side of the grid column header. The numbers represent specific pages, and the advance arrows go one step or all the way forward or back.

To use field sets

Choose a named set of fields from the **Field Set** drop-down menu. The sets available are usually tailored to your enterprise. Note that the field-set variables found in the ArcSight Console are not available through ArcSight Web.

Choose the Field Set **Customize** option (if available) to temporarily add, remove, or rearrange the columns in the current grid. You can create one custom field set per channel.

the Domain Field Sets topic**To sort a grid**

Click any grid column heading to sort the whole view by that column. Each click toggles between ascending and descending. The default order of grids is usually determined by the End Time of events, as selected in the current active channel display.

To filter a grid

To apply an inline filter, click **Inline Filter** in the grid header and choose an available value from the drop-down menus for one or more columns. This enables you to filter by values already available in the channel. Click **Apply** to put the filter into effect.

You can also filter by entering custom expressions into the text field for each column. To customize an inline filter, type a value in the text field above the column on which you want to filter, and click **Apply**. Supported expressions for custom filtering are shown in the table below.

Supported Expressions for Inline Filtering

Type	Supported Expressions and Examples

String-based Columns	The `Contains` and `StartsWith` operators are supported. The values for the operator must be in quotes.
	
	Examples:
	
	`Contains "Event"`
	`Contains "Event" OR Contains "Top"`
	`Contains "Web" AND Contains "denied"`
	`StartsWith "Web"`
	`StartsWith "Web" OR Contains "denied"`
	`StartsWith "Web" AND Contains "denied"`
	You can use OR and AND Boolean operators in between the expressions. The Column field name is implicitly used as the left-hand parameter.

Integer and IP Address Columns	The `Between` operator is supported. The values in the `Between` expression must be in quotes.
	
	Examples:
	
	`For the port column: Between("20", "80")`
	`For the IP address column: Between("10.0.0.1", "10.0.0.255")`
	`For priority column: Between("1","2") OR Between("7","8")`
	You can use OR and AND Boolean operators in between the expressions. The Column field name is implicitly used as the left-hand parameter.

To add an event to a case

Select one or more event check boxes on the left, then click **Add to Case** to choose an existing or new case to add it to in the Cases resource tree. Click the **Existing case** radio button to add the events to the case you select in the tree. Click the **New case** radio button to name the case and add it at the currently selected point in your personal tree. Click **Add** to save the assignments and return to the grid.

To view the events associated with a case, click the Cases navigation button at the top of the page, choose a case, and click the Events tab for that case. For more information, see “Events Tab” on page 99 in “Using Cases” on page 93.

To change a grid's options

Click **Options** in the grid header to change the display's update frequency and its number of rows per page.

To save a modified channel

Click Save Channel As in the channel header to add a modified channel to your personal folder in the Active Channels resource tree. In the Save Channel As dialog box, name the channel and click **Save**.

To inspect an event

Click any individual event in the grid to show that event in the Event Inspector as described in Inspecting Events.

Inspecting Events

Use the Event Inspector display to examine the details of events that appear in active channels. To open the Event Inspector, click an event in an active channel's grid view. The Event Inspector shows the data fields and categories associated with the event you selected. Apart from these fields, the display has the features described below.

Event Inspector Header Features

Feature	Usage
Associated Articles	If a knowledge base article exists for this event, the **View Articles** link will display the article from the Knowledge Base.
Associated References	If a reference page exists for this event, the **View References** link will display the reference page. Reference pages provide additional background on an event or a resource. These may be pre-populated by ArcSight, provided by vendors, or added by technologists in your organization.
Additional Details	Click this link to view **Additional Details** on the event, such as vendor and product information, event category information, reference pages, and vulnerability pages.
View Event Context Report	Click this link to run an **Event Context Report** that shows the events that occurred within a specified number of minutes (a window) before and after this event.
View Rule Context Report	Click this link to run a **Rule Context Report** that shows the events that occurred within a specified number of minutes (a window) before and after the current rule was invoked.
Payload Viewer	Click this link to view the payload for the event. The **Payload Viewer** option is available only if the event has a payload associated with it. A "payload" is information carried in the body of an event's network packet, as distinct from the packet's header data. Events will include payloads only if the associated SmartConnectors are configured to send events with payloads.
View iDefense Incident Report	Click **View iDefense Incident Report** to view information about vulnerability IDs related to the event. This option is available only if you have VeriSign iDefense software installed and configured to interact with the Arcsight system, and if the selected event has a vulnerability ID associated with it. In that case, the iDefense report provides more details on the vulnerability.
Field Sets	Choose **Field Sets** to see a predefined set of event data fields rather than all fields. Use the **None** option to restore the default view.
Hide Empty Rows	By default, the **Hide Empty Rows** check box is checked, so the display isn't filled with unused fields. Clear the check box to see all fields, even if empty.

Event Inspector Field Features

The values for fields in events are also links. Click these values to open new channels or to filter current channels using them.

Option	Use
Create Channel [Field Name = Value]	Open a channel containing only those events that have matching values for the selected field.
Create Channel [Field Name != Value]	Open a channel that shows only those events that do not have a matching value for the selected event.
Add to Channel [Attribute = Value]	Add the attribute-value pair to the channel's filter (require that they match).
Add to Channel [Attribute != Value]	Exclude the attribute-value pair from the channel's filter (require that they do not match).

Show Details for Event Attributes

View details for each attribute associated with an event.

- To view event attribute details inline, click the **Details** button () next to the attribute.
- To view event attribute details on a new Web page, click the **Show detail in a new page** button () next to the attribute.

Event Categories

ESM uses six primary categories and a flexible set of supporting attributes to more precisely distinguish the events reported by SmartConnectors or generated internally by ArcSight Managers. These categories appear as a field in the Event Inspector.

These categories and attributes are designated by ArcSight, based on the information offered to SmartConnectors by sensors. Keep in mind that the applicability of a category always depends on the actual configuration of the environment.

The category groups are:

- **Object**: The physical or virtual object that was the focus of the event. (See “Object Category” on page 24.)
- **Behavior**: The action taken on the object. (See “Behavior Category” on page 25.)
- **Outcome**: An indication of whether the action succeeded on the object. (See “Outcome Category” on page 27.)
- **Device Group**: The type of device from which the sensor reported the event. (See “Device Group Category” on page 27.)
- **Technique**: The method used to apply the action to the object (i.e., the type of attack). (See “Technique Category” on page 28.)
- **Significance**: A description of the security significance of the event from the reporting sensor's perspective. (See “Significance Category” on page 30.)

Object Category

Object Category		Description
Host		Any end-system on the network, such as a PDA, a Windows computer, or a Linux computer.
Operating System		The system software that controls execution of computer programs and access to resources on a host.
Application		A software program that is not an integral part of the operating system.
	Service	An application that normally executes at operating system startup. A service often accepts network connections.
	Database	A database application.
	Backdoor	An application, visible on a host, that listens for network connections and can give a non-authorized user control over that host.
	DoS Client	A host that is displaying an application that can participate in a (possibly distributed) denial-of-service attack.
	Peer to Peer	An application that listens for, and establishes network connections to, other installations of the same application such as Kazaa, Morpheus, or Napster.
	Virus	A host that is displaying a replicating infection of a file that also executes other behaviors on the infected host.
	Worm	A host that is displaying a self-replicating program that spreads itself automatically over the network from one computer to the next.
Resource		An operating system resource that is characteristically limited in its supply.
	File	A long-term storage mechanism (e.g., files, directories, hard disks, etc.).
	Process	A single executable module that runs concurrently with other executable modules.
	Interface	An interface to the network.
	Interface Tunnel	Packaging a lower network protocol layer within a higher layer such as IPSec Tunnel and HTTP tunneling.
	Registry	The central configuration repository for the operating system and the applications. Application-specific information is not stored here.
	CPU	Events directed at this object relate to consumption or use of the overall processing power of the host.
	Memory	Events directed at this object relate to consumption or use of the overall memory of the host.
Network		Events that cannot be clearly associated with a host's subitem. Events that involve transport, or many hosts on the same subnet.

Object Category		Description
	Routing	Routing related events such as BGP.
	Switching	Switching related events such as VLANS.
Actor		
	User	A single human identity.
	Group	A named collection of users, such as an employee division or social group.
Vector		The replication path for a section of malicious code.
	Virus	A replicating infection of a file that also executes other behaviors on the infected host.
	Worm	A self-replicating program that automatically spreads itself across the network, from one computer to the next.
	Backdoor	An application that listens for network connections and can give a non-authorized user control over that host.
	DoS Client	An application that will participate in a (possibly distributed) denial-of-service attack.

Behavior Category

Behavior Category		Description
Access		Refers to accessing objects, as in reading.
	Start	The start of an ongoing access, such as login.
	Stop	The end of an ongoing access, such as logging out.
Authentication		Actions that support authentication.
	Add	Adding new authentication credentials.
	Delete	Deleting authentication credentials.
	Modify	Modifying authentication credentials.
	Verify	Credential verification, such as when logins occur.
Authorization		Authorization-related actions.
	Add	Adding a privilege for the associated object (for example, a user).
	Delete	Removing a privilege for the associated object (for example, a user).
	Modify	Modifying the existing privileges for the associated user or entity.
	Verify	An authorization check, such as a privilege check.
Communicate		Transactions that occur over the wire.

Behavior Category		Description
	Query	Communicating a request to a service.
	Response	Communicating a response to a request, from a service.
Create		Seeks to create resources, install applications or services, or otherwise cause a new instance of an object.
Delete		The reverse of creation events. Includes uninstalling applications, services, or similar activity.
Execute		Involves loading or executing code, booting or shutting systems down, and similar activity.
	Start	The beginning of execution of an application or service. This event is clearly distinguished from a lone "Execute" attribute.
	Stop	The termination of execution of an application or service. This event is clearly distinguished from a lone "Execute" attribute.
	Query	A query sent to a specific entity - but not over the network such as when generating a report.
	Response	The answer returned by an Execute/Query. For example, a report delivered back from an application, or status messages from applications.
Modify		Involves changing some aspect of an object.
	Content	Changing the object's content, such as writing to or deleting from a file or database.
	Attribute	Changing some attribute of an object, such as a file name, modification date, or create date.
	Configuration	Changing an object's configuration. For example, application, operating system, or registry changes.
Substitute		Replacing files, upgrading software, or service or host failovers.
Found		Noticing an object or its state.
	Vulnerable	An exploitable state that is characteristic of a particular hardware or software release.
	Misconfigured	An exploitable state caused by a weak configuration or similar mishandling.
	Insecure	An exploitable state that arises from poor management or implementation. For example, weak authentication, weak passwords, passwords passed in the clear, default passwords, or simplistically named accounts.
	Exhausted	The targeted object was found to be exhausted (for example, not enough file descriptors are available).

Outcome Category

These attributes indicate the probable success or failure of the specified event, within an overall context. For example, the outcome of an event such as an "operation failed" error message can be reported as a "/Success" given that the operation can be presumed to have actually caused a failure. Another example would be an event that identifies a Code Red infection: on a host running Linux the outcome would be "/Failure" (Code Red is Windows-only) while the same event directed at a host with an unknown OS would be reported as an "`/Attempt`.

Outcome Category	Description
Attempt	The event occurred but its success or failure cannot be determined.
Failure	The event can be reasonable presumed to have failed.
Success	The event can be reasonable presumed to have succeeded.

Device Group Category

Device Group Category		Description
Application		An application program.
Assessment Tool		A network- or host-based scanner that monitors issues such as vulnerability, configurations, and ports.
Security Information Manager		A security-event processing correlation engine (such as the Manager). This "device" deals only in correlated events.
Firewall		A firewall.
IDS		An intrusion-detection system.
	Network	A network-based intrusion-detection system.
	Host	A host-based intrusion-detection system.
	Antivirus	An anti-virus scanner.
	File Integrity	A file-integrity scanner.
	Identity Management	Identity management.
	Operating System	An operating system.
Network Equipment		Network equipment.
	Router	A network device with routing (layer 3) capabilities.
	Switches	A network device with switching (layer 2) capabilities.
VPN		A virtual private network.

Technique Category

Technique Category		Description
Traffic		An anomaly in the network traffic, such as non-RFC compliance.
	Network Layer	Anomalies related to IP, ICMP, and other network-layer protocols.
	IP Fragment	Fragmented IP packets.
	Man in the Middle	A man-in-the-middle attack.
	Spoof	Spoofing a source or destination IP address.
	Flow	A problem in network-layer communication logic, such as an out-of-order IP fragment.
	Transport Layer	Anomalies related to TCP, UDP, SSL, and other transport-layer protocols.
	Hijack	Hijacking a connection.
	Spoof	Spoofing a transport layer property such as a TCP port number, or an SSL entity.
	Flow	A problem in TCP connections or flows, such as a SYNACK without SYN, a sequence number mismatch, or time exceeded.
	Application Layer	Application-layer anomalies.
	Flow	A peer does not follow the order of commands.
	Syntax Error	A syntax error in an application-layer command.
	Unsupported Command	A command which does not exist or is not supported.
	Man in the Middle	A man-in-the-middle attack on the application layer.
Exploit	**Vulnerability**	Exploiting a vulnerability such as a buffer overflow, code injection, or format string.
	Weak Configuration	Exploitation of a weak configuration. This is something that could be remedied easily by changing the configuration of the service Examples of a weak configuration are weak passwords, default passwords, insecure software versions, or open SMTP relays.
	Privilege Escalation	A user identity has received an increase in its user privileges.
	Directory Transversal	A user identity is attempting to browse or methodically review directories for which it may not have appropriate privileges.
	Brute Force	Brute-force attacks.
	Login	Continued trials for logins.
	URL Guessing	Continued trials for URLs to access information or scripts.
	Redirection	Redirecting an entity.

Technique Category		Description
	ICMP	ICMP redirects.
	DNS	Unauthorized DNS changes.
	Routing Protocols	Attacks aimed at routing protocols such as BGP, RIP, and OSPF.
	IP	Redirection using the IP protocol (source routing).
	Application	Redirection attacks on the application layer such as cross-site scripting, mail routing, or JavaScript spoofing.
	Code Execution	Either the execution or transmission of executable code, or the transmission of a distinctive response from executed code.
	Trojan	The code in question is concealed within other code that serves as a Trojan Horse. In other words, it appears to be one thing (that is safe) but is really another (which is unsafe).
	Application Command	The code in question is intended to invoke an application command.
	Shell Command	The code in question is intended to be executed in a shell.
	Worm	Code associated with a worm.
	Virus	Code associated with a virus.
	Scan	Any type of scanning. A network, host, application, or operating system scan can be identified through the specified object.
	Port	Multiple ports are scanned.
	Service	A service is scanned (for example, DoS client discovery, backdoors, RPC services, or scans for a specific application such as NMB).
	Host	Scanning for hosts on a network.
	IP Protocol	A search for responding protocols. Note that TCP and UDP are not the only transport protocols available.
	Vulnerability	A scan for vulnerabilities.
DoS		A denial of service (DoS) attack is in progress.
Information Leak		Information leaking out of its intended environment such as mail messages leaking out, system file access, FTP data access, or web document access.
	Convert Channel	Leakage was detected from a covert channel such as Loki.
Policy		Policy-related violations such as pornographic web site access.
	Breach	A policy-related security breach occurred.
	Compliant	A policy-compliant event occurred.

Significance Category

Significance Category		Description
Compromise		A potentially compromising event occurred.
Hostile		A malicious event has happened or is happening.
Informational		Events considered worthy of inspection; for example, those produced by polling.
	Error	An execution problem.
	Warning	A possible problem.
	Alert	A situational problem that requires immediate attention.
Normal		Ordinary or expected activity that is significant only for forensic purposes.
Recon		Relates to scans and other reconnaissance activity.
Suspicious		A potentially malicious event occurred.

Event Data Fields

The security monitoring devices report events that are collected, filtered, and formatted by ArcSight SmartConnectors and passed to Managers for analysis. The events that appear in your client are composed of several data fields, each of which has its own characteristics.

Event data fields fall into the groups shown below. Most groups have several attributes.

- Connector
- Attacker
- Category
- Destination
- Device
- Device Custom
- Event
- Event Annotation
- File
- Final Device
- Flex
- Manager
- Old File
- Original Agent
- Request
- Source
- Target
- Threat

Connector

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Agent** (agents are also known as SmartConnectors). Although the Original Agent is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the ArcSight Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Address	connectorAddress	IP address	1	The IP address of the device hosting the SmartConnector.
Connector	Asset ID	connectorAssetId	Resource	1	The asset that represents the device hosting the SmartConnector.
Connector	Asset Name	connectorAssetName	String	1	The connector's asset name.
Connector	Asset Resource	connectorAssetResource	Resource	1	The connector resource.
Connector	Descriptor ID	connectorDescriptorId	ID	1	The connector descriptor.
Connector	DNS Domain	connectorDnsDomain	String	1	The Domain Name Service domain name associated with the device hosting the SmartConnector.
Connector	Host Name	connectorHostName	String	1	The name of the device hosting the SmartConnector.
Connector	ID	connectorId	String	1	The identifier associated with the SmartConnector configuration resource. The format is connectorID(1) | connectorID(2) | ...
Connector	MAC Address	connectorMacAddress	MacAddress	1	The MAC address associated with the SmartConnector (which may or may not be the MAC address of the host device.)

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Name	connectorName	String	1	The user-supplied name of the associated SmartConnector configuration resource.
Connector	NT Domain	connectorNtDomain	String	1	The Windows NT domain associated with the device hosting the SmartConnector.
Connector	Receipt Time	connectorReceiptTime	DateTime	2	The time the event arrived at the SmartConnector.
Connector	Severity	connectorSeverity	Connector Severity Enumeration	1	The normalized ArcSight form of the event severity value provided by the SmartConnector.
Connector	Time Zone	connectorTimeZone	String	1	The time zone reported by the device hosting the SmartConnector (as TLA).
Connector	Time Zone Offset	connectorTimeZoneOffset	Integer	1	The time zone reported by the device hosting the SmartConnector (shown as a UTC offset). Note that device times may be less accurate than other sources.
Connector	Translated Address	connectorTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the SmartConnector.
Connector	Translated Zone	connectorTranslatedZone	Zone	1	If network address translation is an issue, this is the Network Zone associated with the translated IP address of the device hosting the SmartConnector.
Connector	Translated Zone External ID	connectorTranslatedZoneExternalID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Translated Zone ID	connectorTranslatedZoneID	String	1	See the common set of resource attributes.
Connector	Translated Zone Name	connectorTranslatedZoneName	String	1	See the common set of resource attributes. Returns the name from the URI. It assumes that the name is always the last field of the URI.
Connector	Translated Zone Reference ID	connectorTranslatedZoneReferenceID	ID	1	See the common set of resource attributes. Returns the unique descriptor ID for this reference.
Connector	Translated Zone Resource	connectorTranslatedZoneResource	Resource	1	See the common set of resource attributes. Locates the resource described by this reference.
Connector	Translated Zone URI	connectorTranslatedZoneURI	String	1	See the common set of resource attributes.
Connector	Type	connectorType	String	1	A description of the type of SmartConnector that reported the event.
Connector	Version	connectorVersion	String	1	The software revision number of the SmartConnector that reported the event
Connector	Zone	connectorZone	Zone	1	The network zone in which the device hosting this SmartConnector resides.
Connector	Zone External ID	connectorZoneExternalID	String	1	See the common set of resource attributes.
Connector	Zone ID	connectorZoneID	String	1	See the common set of resource attributes.
Connector	Zone Name	connectorZoneName	String	1	See the common set of resource attributes.
Connector	Zone Reference ID	connectorZoneReferenceID	ID	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Zone Resource	connectorZoneResource	Resource	1	See the common set of resource attributes.
Connector	Zone URI	connectorZoneURI	String	1	Returns the URI for this reference.

Attacker

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Address	attackerAddress	IP address	1	The IP address of the device hosting the attacker.
Attacker	Asset ID	attackerAssetId	Resource	2	The asset that represents the device hosting the attacker.
Attacker	Asset Name	attackerAssetName	String	2	The name of the asset that represents the device hosting the attacker.
Attacker	Asset Resource	attackerAssetResource	Resource	2	See the common set of resource attributes
Attacker	DNS Domain	attackerDnsDomain	String	2	The Domain Name Service domain name associated with the device hosting the attacker.
Attacker	FQDN	attackerFqdn	String	2	The fully qualified domain name associated with the device hosting the attacker.
Attacker	Geo	attackerGeo	GeoDescriptor	1	See the common set of geographical attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Geo Country Code	attackerGeoCountryCode	String	1	See the common set of geographical attributes.
Attacker	Geo Country Flag URL	attackerGeoCountryFlagUrl	String	1	See the common set of geographical attributes.
Attacker	Geo Country Name	attackerGeoCountryName	String	1	See the common set of geographical attributes.
Attacker	Geo Descriptor ID	attackerGeoDescriptorId	ID	1	See the common set of geographical attributes.
Attacker	Geo Latitude	attackerGeoLatitude	Double	1	See the common set of geographical attributes.
Attacker	Geo Location Info	attackerGeoLocationInfo	String	Location	See the common set of geographical attributes.
Attacker	Geo Longitude	attackerGeoLongitude	Double	1	See the common set of geographical attributes.
Attacker	Geo Postal Code	attackerGeoPostalCode	String	1	See the common set of geographical attributes.
Attacker	Geo Region Code	attackerGeoRegionCode	String	1	See the common set of geographical attributes.
Attacker	Host Name	attackerHostName	String	2	The name of the device hosting the attacker.
Attacker	MAC Address	attackerMacAddress	MAC address	2	The MAC address associated with the source of the attack (which may or may not be the MAC address of the host device).
Attacker	NT Domain	attackerNtDomain	String	2	The Windows NT domain associated with the device hosting the attacker.
Attacker	Port	attackerPort	Integer	1	The network port associated with the source of the attack.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Process Name	attackerProcessName	String	2	The name of process associated with the source of the attack.
Attacker	Service Name	attackerServiceName	String	2	The name of service associated with the source of the attack.
Attacker	Translated Address	attackerTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the attacker.
Attacker	Translated Port	attackerTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack. This can happen in a NAT environment.
Attacker	Translated Zone	attackerTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device hosting the attacker.
Attacker	Translated Zone External ID	attackerTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Attacker	Translated Zone ID	attackerTranslatedZoneID	String	1	See the common set of resource attributes.
Attacker	Translated Zone Name	attackerTranslatedZoneName	String	1	See the common set of resource attributes. It is assumed that the name is always the last field of the URI.
Attacker	Translated Zone Reference ID	attackerTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.
Attacker	Translated Zone Resource	attackerTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Attacker	Translated Zone URI	attackerTranslatedZoneURI	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	User ID	attackerUserId	String	2	The identifier associated with the OS or application of the attacker, at the source of the attack.
Attacker	User Name	attackerUserName	String	2	The name associated with the attacker, at the source of the attack.
Attacker	User Privileges	attackerUserPrivileges	String	2	The user-privilege associated with the attacker, at the source of the attack.
Attacker	Zone	attackerZone	Zone	1	The network zone in which the attacker's device resides.
Attacker	Zone External ID	attackerZoneExternalID	String	1	See the common set of resource attributes.
Attacker	Zone ID	attackerZoneID	String	1	See the common set of resource attributes.
Attacker	Zone Name	attackerZoneName	String	1	See the common set of resource attributes. It is assumed that the name is always the last field of the URI.
Attacker	Zone Reference ID	attackerZoneReferenceID	ID	1	See the common set of resource attributes.
Attacker	Zone Resource	attackerZoneResource	Resource	1	See the common set of resource attributes.
Attacker	Zone URI	attackerZoneURI	String	1	See the common set of resource attributes.

Category

See “Event Categories” on page 23 for a complete description of the event category types and their supporting attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Category	Behavior	categoryBehavior	String	1	Describes the action taken with or by the object.
Category	Custom Format Field	categoryCustomFormatField	String	1	Describes the content of a custom formatted field, if present.
Category	Descriptor ID	categoryDescriptorId	ID	1	The unique ID for the sensor that reported the event
Category	Device Group	categoryDeviceGroup	String	1	Describes the type of event this event represents.
Category	Object	categoryObject	String	1	Describes the physical or virtual object that was the focus of the event
Category	Outcome	categoryOutcome	String	1	Indicates whether the action was successfully applied to the object.
Category	Significance	categorySignificance	String	1	Characterizes the event from a network-intrusion-detection perspective.
Category	Technique	categoryTechnique	String	1	Describes the method used to apply the action to the object.
Category	Tuple Description	categoryTupleDescription	String	1	The prose description of the event category, assembled from the category components.

Destination

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Address	destinationAddress	IP address	1	The IP address of the destination device.
Destination	Asset ID	destinationAssetId	Resource	2	The asset that represents the device that was the network traffic's destination.
Destination	Asset Name	destinationAssetName	String	2	See the common set of resource attributes.
Destination	Asset Resource	destinationAssetResource	Resource	2	See the common set of resource attributes.
Destination	DNS Domain	destinationDnsDomain	String	2	The Domain Name Service domain name associated with the user at the destination device.
Destination	FQDN	destinationFqdn	String	2	The fully qualified domain name associated with the destination device.
Destination	Geo	destinationGeo	GeoDescriptor		See the common set of geographical attributes.
Destination	Geo Country Code	destinationGeoCountryCode	String	1	The country code.
Destination	Geo Country Flag URL	destinationGeoCountryFlagUrl	String	1	The country flag.
Destination	Geo Country Name	destinationGeoCountryName	String	1	The country name.
Destination	Geo Descriptor ID	destinationGeoDescriptorId	ID	1	See the common set of geographical attributes.
Destination	Geo Latitude	destinationGeoLatitude	Double	1	The destination latitude.
Destination	Geo Location Info	destinationGeoLocationInfo	String	1	The destination location.
Destination	Geo Longitude	destinationGeoLongitude	Double	1	The destination longitude.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Geo Postal Code	destinationGeoPostalCode	String	1	The destination postal code.
Destination	Geo Region Code	destinationGeoRegionCode	String	1	See the common set of geographical attributes.
Destination	Host Name	destinationHostName	String	2	The name of the destination device.
Destination	MAC Address	destinationMacAddress	MAC address	2	The MAC address associated with the network traffic's destination (which may or may not be the MAC address of the host device).
Destination	NT Domain	destinationNtDomain	String	2	The Windows NT domain associated with the destination device.
Destination	Port	destinationPort	Integer	1	The network port associated with the network traffic's destination.
Destination	Process Name	destinationProcessName	String	2	The name of process associated with the network traffic's destination.
Destination	Service Name	destinationServiceName	String	2	The name of service associated with the network traffic's destination.
Destination	Translated Address	destinationTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device that was the network traffic's destination.
Destination	Translated Port	destinationTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Translated Zone	destinationTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device at the network's traffic's destination.
Destination	Translated Zone External ID	destinationTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Destination	Translated Zone ID	destinationTranslatedZoneID	String	1	See the common set of resource attributes.
Destination	Translated Zone Name	destinationTranslatedZoneName	String	1	See the common set of resource attributes.
Destination	Translated Zone Reference	destinationTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.
Destination	Translated Zone Resource	destinationTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Destination	Translated Zone URI	destinationTranslatedZoneURI	String	1	See the common set of resource attributes.
Destination	User ID	destinationUserId	String	2	The OS- or application-based identifier associated with the user at the network traffic's destination.
Destination	User Name	destinationUserName	String	2	The name associated with the user at the network traffic's destination.
Destination	User Privileges	destinationUserPrivileges	String	2	The privileges accorded the user at the network traffic destination.
Destination	Zone	destinationZone	Zone	1	The network zone in which the destination device resides.
Destination	Zone External ID	destinationZoneExternalID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Zone ID	destinationZoneID	String	1	See the common set of resource attributes.
Destination	Zone Name	destinationZoneName	String	1	See the common set of resource attributes.
Destination	Zone Reference ID	destinationZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Destination	Zone Resource	destinationZoneResource	Resource	1	See the common set of resource attributes.
Destination	Zone URI	destinationZoneURI	String	1	See the common set of resource attributes.

Device

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Action	deviceAction	String	2	The device-specific description of some activity associated with the event
Device	Address	deviceAddress	IP address	1	The IP address of the device hosting the sensor.
Device	Asset ID	deviceAssetId	Resource	1	The asset that represents the device hosting the sensor.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Asset Name	deviceAssetName	String	1	The name of the device.
Device	Asset Resource	deviceAssetResource	Resource	1	The resource the asset represents.
Device	Descriptor ID	deviceDescriptorId	ID	1	The asset's descriptor ID.
Device	Direction	deviceDirection	DeviceDirectionEnumeration	2	Whether the traffic was inbound or outbound.
Device	DNS Domain	deviceDnsDomain	String	1	The Domain Name Service domain name associated with the device hosting the sensor.
Device	Domain	deviceDomain	String	2	The specific domain containing the sensor device associated with the event
Device	Event Category	deviceEventCategory	String	2	The category description included with the event as reported by the device.
Device	Event Class ID	deviceEventClassId	String	2	The device-specific identifier associated with this type of event
Device	External ID	deviceExternalId	String	1	The external identifier associated with this sensor device, if provided by the vendor.
Device	Facility	deviceFacility	String	1	The sensor submodule that reported the event
Device	Host Name	deviceHostName	String	1	The name of the device hosting the sensor.
Device	Inbound Interface	deviceInboundInterface	String	1	The NIC card on the sensor device that received the network traffic associated with the event.
Device	MAC Address	deviceMacAddress	MAC address	1	The MAC address associated with the source of the attack (which may or may not be the MAC address of the host device).

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	NT Domain	deviceNtDomain	String	1	The Windows NT domain associated with the device hosting the sensor.
Device	Outbound Interface	deviceOutboundInterface	String	1	The NIC card on the sensor device that transmitted the network traffic associated with the event.
Device	Payload ID	devicePayloadId	String	2	The internal identifier associated with a payload object associated with this event.
Device	Process Name	deviceProcessName	String	1	The sensor device process that reported the event.
Device	Product	deviceProduct	String	1	The product name of the sensor device.
Device	Receipt Time	deviceReceiptTime	DateTime	2	The time when the sensor device observed the event.
Device	Severity	deviceSeverity	String	2	The device-specific assessment of event severity. This assessment varies with the device involved.
Device	Time Zone	deviceTimeZone	String	1	The time zone reported by the device hosting the sensor device (shown as TLA).
Device	Time Zone Offset	deviceTimeZoneOffset	Integer	1	The time zone reported by the device hosting this sensor device (shown as an offset from UTC).
Device	Translated Address	deviceTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the sensor.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Translated Zone	deviceTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device hosting the sensor.
Device	Translated Zone External ID	deviceTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Device	Translated Zone ID	deviceTranslatedZoneID	String	1	See the common set of resource attributes.
Device	Translated Zone Name	deviceTranslatedZoneName	String	1	See the common set of resource attributes.
Device	Translated Zone Resource	deviceTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Device	Translated Zone Resource	deviceTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Device	Translated Zone URI	deviceTranslatedZoneURI	String	1	See the common set of resource attributes.
Device	Vendor	deviceVendor	String	1	The vendor who manufactured or sold the sensor device.
Device	Version	deviceVersion	String	1	The software revision number of the sensor device.
Device	Zone	deviceZone	Zone	1	The network zone in which the sensor's device resides.
Device	Zone External ID	deviceZoneExternalID	String	1	See the common set of resource attributes.
Device	Zone ID	deviceZoneID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Zone Name	deviceZoneName	String	1	See the common set of resource attributes.
Device	Zone Reference ID	deviceZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been persisted and given a unique database identifier.
Device	Zone Resource	deviceZoneResource	Resource	1	See the common set of resource attributes.
Device	Zone URI	deviceZoneURI	String	1	See the common set of resource attributes.

Device Custom

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device Custom	Date1	deviceCustomDate1	DateTime	2	First customDate
Device Custom	Date1 Label	deviceCustomDate1Label	String	2	First customDate label
Device Custom	Date2	deviceCustomDate2	DateTime	2	Second customDate
Device Custom	Date2 Label	deviceCustomDate2Label	String	2	Second customDate label
Device Custom	Descriptor ID	deviceCustomDescriptorId	ID	2	Custom descriptior ID
Device Custom	Number1	deviceCustomNumber1	Long	2	First customNumber
Device Custom	Number1 Label	deviceCustomNumber1Label	String	2	First customNumber label

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device Custom	Number2	deviceCustomNumber2	Long	2	Second customNumber
Device Custom	Number2 Label	deviceCustomNumber2Label	String	2	Second customNumber label
Device Custom	Number3	deviceCustomNumber3	Long	2	Third customNumber
Device Custom	Number3 Label	deviceCustomNumber3Label	String	2	Third customNumber label
Device Custom	String1	deviceCustomString1	String	2	First customString
Device Custom	String1 Label	deviceCustomString1Label	String	2	First customString label
Device Custom	String2	deviceCustomString2	String	2	Second customString
Device Custom	String2 Label	deviceCustomString2Label	String	2	Second customString label
Device Custom	String3	deviceCustomString3	String	2	Third customString
Device Custom	String3 Label	deviceCustomString3Label	String	2	Third customString label
Device Custom	String4	deviceCustomString4	String	2	Fourth customString
Device Custom	String4 Label	deviceCustomString4Label	String	2	Fourth customString label
Device Custom	String5	deviceCustomString5	String	2	Fifth customString
Device Custom	String5 Label	deviceCustomString5Label	String	2	Fifth customString label
Device Custom	String6	deviceCustomString6	String	2	Sixth customString
Device Custom	String6 Label	deviceCustomString6Label	String	2	Sixth customString label

Event

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Additional Data	additionalData	AdditionalData	3	Reference to additional data.
Event	Aggregated Event Count	(not applicable)	(not applicable)	n/a	A derived field that reports the number of actual events collectively represented by the event in question.
Event	Application Protocol	applicationProtocol	String	2	A description of the application layer protocol. May be set, but defaults to Target Port lookup (FTP).
Event	Base Event Count	baseEventCount	Integer	1	The number of events upon which this event is based (e.g., type == BASE|ACTION).
Event	Base Event IDs	baseEventIds	ID	2	The array of event IDs that contributed to generating this correlation event. This is populated only in correlated events.
Event	Bytes In	bytesIn	Integer	2	Number of bytes transferred into the device during this transaction (this would typically be associated with entries in HTTP logs).
Event	Bytes Out	bytesOut	Integer	2	Number of bytes transferred out of the device during this transaction (this would typically be associated with entries in HTTP logs).
Event	Concentrator Connectors	concentratorConnectors	ConnectorDescriptor	2	The chain of concentrators that forwarded the event This is not yet exposed in the user interface.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Concentrator Devices	concentratorDevices	DeviceDescriptor	2	The list of devices that concentrate events, if applicable. This is not exposed in the user interface.
Event	Correlated Event Count	(not applicable)	(not applicable)	n/a	A derived field that reports the number of actual events that had to occur to cause a correlation event to occur.
Event	Crypto Signature	cryptoSignature	String	2	The signature of the event object (meaning in this alert, as opposed to the occurrence represented by the event). Not yet supported.
Event	Customer	customer	Customer	1	The "customer" resource reference. This is used in MSSP environments to describe the client or divisional entity to whom the event applies.
Event	Customer External ID	customerExternalID	String	1	Returns the external ID for this reference.
Event	Customer ID	customerID	String	1	Returns the ID for the resource in this resource reference.
Event	Customer Name	customerName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event	Customer Reference ID	customerReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event	Customer Resource	customerResource	Resource	1	Locates the resource described by this reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Customer URI	customerURI	String	1	Returns the URI for this reference.
Event	End Time	endTime	DateTime	1	Event ends (defaults to deviceReceiptTime).
Event	Event ID	eventId	ID	1	Long value identifying an event.
Event	External ID	externalId	String	2	A reference to the ID used by an external device. This is useful for tracking devices that create events that contain references to these IDs (e.g., ManHunt).
Event	Generator	generator	null	1	The "generator" resource reference (the resource that generated the event. This is the subcomponent in the connector that generates the event.
Event	Generator External ID	generatorExternalID	String	1	Returns the external ID for this reference.
Event	Generator ID	generatorID	String	1	Returns the ID for the resource in this resource reference.
Event	Generator Name	generatorName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event	Generator Reference ID	generatorReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event	Generator Resource	generatorResource	Resource	1	Locates the resource described by this reference.
Event	Generator URI	generatorURI	String	1	Returns the URI for this reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Locality	locality	LocalityEnumeration	2	The locality associated with the event.
Event	Message	message	String	2	A brief comment associated with this event.
Event	Name	name	String	1	An arbitrary string that describes this type of event. Event details included in other parts of an event shouldn't be used in the event name.
Event	Originator	originator	OriginatorEnumeration	1	Holds the value of Source|Destination. This determines whether source and destination should be translated to attacker and target or they should be inversed.
Event	Persistence	persistence	PersistenceEnumeration	2	There are two states: Persisted or Transient. Events default to being Transient and are marked as Persisted as soon as they reach the Batch Alert Persistor or when they are loaded by the Alert Broker.
Event	Raw Event	rawEvent	String	1	The original log entry reported by the sensor (synthesized when the sensor does not log to a file or text stream).
Event	Rule Thread ID	ruleThreadId	String	2	A single rule can issue many events, based on several triggers, starting with On First Event and ending with On Threshold Timeout. All such events for a single Rule and a single Group By tuple will be marked with the same identifier using this attribute.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Session ID	sessionId	Long	2	Tags for events created by a correlation simulation, as part of a particular simulation.
Event	Start Time	startTime	DateTime	1	Event begins (defaults to deviceReceiptTime).
Event	Transport Protocol	transportProtocol	String	1	The format of the transmitted data associated with the event from a network transport perspective (e.g., TCP, UDP).
Event	Type	type	TypeEnumeration	1	One of the event types: Base, Correlation, Aggregation, or Action.
Event	Vulnerability	vulnerability	Vulnerability	2	The vulnerability resource that represents the vulnerability or exposure that may be exploited by this event and is present on the targeted device according to our network model.
Event	Vulnerability External ID	vulnerabilityExternalID	String	2	Returns the external ID for this reference.
Event	Vulnerability ID	vulnerabilityID	String	2	Returns the ID for the resource in this resource reference.
Event	Vulnerability Name	vulnerabilityName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event	Vulnerability Reference ID	vulnerabilityReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event	Vulnerability Resource	vulnerabilityResource	Resource	2	Locates the resource described by this reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Vulnerability URI	vulnerabilityURI	String	2	Returns the URI for this reference.

Event Annotation

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Audit Trail	eventAnnotationAuditTrail	String	2	The text log of annotation changes. Changes are recorded as sets of comma-separated-value entries.
Event Annotation	Comment	eventAnnotationComment	String	2	A text description of the event or associated information.
Event Annotation	End Time	eventAnnotationEndTime	DateTime	2	The timestamp for an eventannotation.
Event Annotation	Event ID	eventAnnotationEventId	ID	2	The event ID for the annotation event.
Event Annotation	Flags	eventAnnotationFlags	FlagsValueSet	2	The state of the collaboration flags.
Event Annotation	Manager Receipt Time	eventAnnotationManagerReceiptTime	DateTime	2	The time the Manager received the event annotation.
Event Annotation	Modification Time	eventAnnotationModificationTime	DateTime	2	The time the annotation was modified.
Event Annotation	Modified By	eventAnnotationModifiedBy	User	2	The user ID of the person who last edited this annotation.
Event Annotation	Modified By External ID	eventAnnotationModifiedByExternalID	String	2	Returns the external ID for this reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Modified By ID	eventAnnotationModifiedByID	String	2	Returns the ID for the resource in this resource reference.
Event Annotation	Modified By Name	eventAnnotationModifiedByName	String	2	Returns the name from the URI (the last field of the URI).
Event Annotation	Modified By Reference ID	eventAnnotationModifiedByReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event Annotation	Modified By Resource	eventAnnotationModifiedByResource	Resource	2	Locates the resource described by this reference.
Event Annotation	Modified By URI	eventAnnotationModifiedByURI	String	2	Returns the URI for this reference.
Event Annotation	Stage	eventAnnotationStage	Stage	2	The current disposition of the event. This enables annotation workflow.
Event Annotation	Stage Event ID	eventAnnotationStageEventId	ID	2	The reference to an internal identifier for another event. It is used by 'Mark Similar'.
Event Annotation	Stage External ID	eventAnnotationStageExternalID	String	2	Returns the external ID for this reference.
Event Annotation	Stage ID	eventAnnotationStageID	String	2	Returns the ID for the resource in this resource reference.
Event Annotation	Stage Name	eventAnnotationStageName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event Annotation	Stage Reference ID	eventAnnotationStageReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference is stored and uniquely identified in the database.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Stage Resource	eventAnnotationStageResource	Resource	2	Locates the resource described by this reference.
Event Annotation	Stage Update Time	eventAnnotationStageUpdateTime	ID	2	The time of the last stage change (in UTC).
Event Annotation	Stage URI	eventAnnotationStageURI	String	2	Returns the URI for this reference.
Event Annotation	Stage User	eventAnnotationStageUser	User	2	The user associated with the current stage. This implements assignment within workflow.
Event Annotation	Stage User External ID	eventAnnotationStageUserExternalID	String	2	Returns the external ID for this reference.
Event Annotation	Stage User ID	eventAnnotationStageUserID	String	2	Returns the ID for the resource in this resource reference.
Event Annotation	Stage User Name	eventAnnotationStageUserName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event Annotation	Stage User Reference ID	eventAnnotationStageUserReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference is stored and uniquely identified in the database.
Event Annotation	Stage User Resource	eventAnnotationStageUserResource	Resource	2	Locates the resource described by this reference.
Event Annotation	Stage User URI	eventAnnotationStageUserURI	String	2	Returns the URI for this reference.
Event Annotation	Version	eventAnnotationVersion	Integer	2	The editing version number which increments with each change. This enables optimistic locking.

File

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
File	Create Time	fileCreateTime	DateTime	2	The time the file was created (in UTC).
File	Hash	fileHash	String	2	The hashcode associated with the file's contents (e.g., MD5).
File	ID	fileId	String	2	The external identifier associated with the file.
File	Modification Time	fileModificationTime	DateTime	2	The time the file was last changed (in UTC).
File	Name	fileName	String	2	The name of the file.
File	Path	filePath	String	2	The directory path to the file in the file system.
File	Permission	filePermission	String	2	The user permissions associated with the file (sensor specific).
File	Size	fileSize	Long	2	The size of the file's contents (typically in bytes; sensor specific).
File	Type	fileType	String	2	The type of file contents (sensor specific).

Final Device

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Address	finalDeviceAddress	IP address	2	The IP address of the trusted reporting device.
Final Device	Asset ID	finalDeviceAssetId	Resource	2	The asset that represents the trusted reporting device.
Final Device	Asset Name	finalDeviceAssetName	String	2	The name of the trusted reporting device.
Final Device	Asset Resource	finalDeviceAssetResource	Resource	2	The resource represented by the trusted reporting device.
Final Device	Descriptor ID	finalDeviceDescriptorId	ID	2	The descriptor ID of the trusted reporting device.
Final Device	DNS Domain	finalDeviceDnsDomain	String	2	The Domain Name Service domain name associated with the trusted reporting device.
Final Device	External ID	finalDeviceExternalId	String	2	The external ID for the trusted reporting device, if provided by the vendor.
Final Device	Facility	finalDeviceFacility	String	2	A facility or capability of a device. This accomodates concentrators (e.g., like syslog, which has a concept of device logging for "parts" of a device).
Final Device	Host Name	finalDeviceHostName	String	2	The host name of the trusted reporting device.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Inbound Interface	finalDeviceInboundInterface	String	2	The NIC card on the sensor device that received the network traffic associated with the event.
Final Device	MAC address	finalDeviceMacAddress	MAC address	2	The MAC address associated with the trusted reporting device.
Final Device	NT Domain	finalDeviceNtDomain	String	2	The Windows NT domain associated with the trusted reporting device.
Final Device	Outbound Interface	finalDeviceOutboundInterface	String	2	The NIC card on the trusted reporting device.
Final Device	Process Name	finalDeviceProcessName	String	2	The process name of the trusted reporting device.
Final Device	Product	finalDeviceProduct	String	2	The product name of the trusted reporting device.
Final Device	Time Zone	finalDeviceTimeZone	String	2	The time zone reported by the trusted reporting device.
Final Device	Time Zone Offset	finalDeviceTimeZoneOffset	Integer	2	Returns the raw time-zone offset for the trusted reporting device. Note that connector and device times are not always reliably accurate.
Final Device	Translated Address	finalDeviceTranslatedAddress	IP address	2	If network address translation is an issue, this is the translated IP address of the trusted reporting device.
Final Device	Translated Zone	finalDeviceTranslatedZone	Zone	2	If network address translation is an issue, this is the network zone associated with the translated IP address of the trusted reporting device.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Translated Zone External ID	finalDeviceTranslatedZoneExternalID	String	2	Returns the external ID for this reference.
Final Device	Translated Zone ID	finalDeviceTranslatedZoneID	String	2	Returns the ID for the resource in this resource reference.
Final Device	Translated Zone Name	finalDeviceTranslatedZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Final Device	Translated Zone Reference ID	finalDeviceTranslatedZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Final Device	Translated Zone Resource	finalDeviceTranslatedZoneResource	Resource	2	Locates the resource described by this reference.
Final Device	Translated Zone URI	finalDeviceTranslatedZoneURI	String	2	Returns the URI for this reference.
Final Device	Vendor	finalDeviceVendor	String	2	Device vendor.
Final Device	Version	finalDeviceVersion	String	2	The software revision number of the trusted reporting device.
Final Device	Zone	finalDeviceZone	Zone	2	The network zone in which the trusted reporting device resides.
Final Device	Zone External ID	finalDeviceZoneExternalID	String	2	Returns the external ID for this reference.
Final Device	Zone ID	finalDeviceZoneID	String	2	Returns the ID for the resource in this resource reference.
Final Device	Zone Name	finalDeviceZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Zone Reference ID	finalDeviceZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Final Device	Zone Resource	finalDeviceZoneResource	Resource	2	Locates the resource described by this reference.
Final Device	Zone URI	finalDeviceZoneURI	String	2	Returns the URI for this reference.

Flex

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Flex	Date1	flexDate1	DateTime	2	First flexDate.
Flex	Date1 Label	flexDate1Label	String	2	Label of first flexDate.
Flex	Number1	flexNumber1	Long	2	First flexNumber.
Flex	Number1 Label	flexNumber1Label	String	2	Label of the first FlexNumber.
Flex	Number2	flexNumber2	Long	2	Second flexNumber.
Flex	Number2 Label	flexNumber2Label	String	2	Label of the second FlexNumber.
Flex	String1	flexString1	String	2	First flexString
Flex	String1 Label	flexString1Label	String	2	Label of the first FlexString.
Flex	String2	flexString2	String	2	Second flexString.
Flex	String2 Label	flexString2Label	String	2	Label of the second FlexString.

Manager

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Manager	Receipt Time	managerReceiptTime	DateTime	1	The time at which the current Manager first received the event.

Old File

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Old File	Create Time	oldFileCreateTime	DateTime	2	The time the file was created (in UTC).
Old File	Hash	oldFileHash	String	2	The hashcode associated with the file's contents (e.g., MD5).
Old File	ID	oldFileId	String	2	The external identifier associated with the file.
Old File	Modification Time	oldFileModificationTime	DateTime	2	The time the file was last changed (in UTC).
Old File	Name	oldFileName	String	2	The file's name.
Old File	Path	oldFilePath	String	2	The directory path to the file in the file system.
Old File	Permission	oldFilePermission	String	2	The user permissions associated with the file (sensor specific).
Old File	Size	oldFileSize	Long	2	The size of the file's contents (typically in bytes; sensor specific).
Old File	Type	oldFileType	String	2	The type of the file's contents (sensor specific).

Original Connector

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original Connector	Address	originalConnectorAddress	IP address	2	The IP address of the device hosting the first reporting SmartConnector.
Original Connector	Asset ID	originalConnectorAssetID	Resource	2	The asset that represents the device hosting the first reporting SmartConnector.
Original Connector	Asset Name	originalConnectorAssetName	String	2	The first reporting connector's asset name.
Original Connector	Asset Resource	originalConnectorAssetResource	Resource	2	The first reporting connector's resource.
Original Connector	Descriptor ID	originalConnectorDescriptorId	ID	2	The first reporting connector's descriptor.
Original Connector	DNS Domain	originalConnectorDnsDomain	String	2	The Domain Name Service domain name associated with the device hosting the first reporting SmartConnector.
Original Connector	Host Name	originalConnectorHostName	String	2	The name of the device hosting the first reporting SmartConnector.
Original Connector	ID	originalConnectorId	String	2	The ID of the connector. The format is connectorId(1)|connectorId(2)|...

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original connector	MAC address	originalconnectorMacAddress	MAC address	2	The MAC address associated with the first reporting Smartconnector (which may or may not be the MAC address of the host device.)
Original connector	Name	originalconnectorName	String	2	User-supplied name of the first reporting connector.
Original connector	NT Domain	originalconnectorNtDomain	String	2	The Windows NT domain associated with the device hosting the first reporting Smartconnector.
Original connector	Time Zone	originalconnectorTimeZone	String	2	The time zone reported by the device hosting the first reporting Smartconnector.
Original connector	Time Zone Offset	originalconnectorTimeZoneOffset	Integer	2	Returns the raw time-zone offset for the first reporting connector's time zone. Note that device and connector times may not be reliably accurate.
Original connector	Translated Address	originalconnectorTranslatedAddress	IP address	2	If network address translation is an issue, this is the translated IP address of the device hosting the first reporting Smartconnector.
Original connector	Translated Zone	originalconnectorTranslatedZone	Zone	2	If network address translation is an issue, this is the Network Zone associated with the translated IP address of the device hosting the first reporting Smartconnector.
Original connector	Translated Zone External ID	originalconnectorTranslatedZoneExternalID	String	2	Returns the external ID for this reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original connector	Translated Zone ID	originalconnectorTranslatedZoneID	String	2	Returns the ID for the resource in this resource reference.
Original connector	Translated Zone Name	originalconnectorTranslatedZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Original connector	Translated Zone Reference ID	originalconnectorTranslatedZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Original connector	Translated Zone Resource	originalconnectorTranslatedZoneResource	Resource	2	Locates the resource described by this reference.
Original connector	Translated Zone URI	originalconnectorTranslatedZoneURI	String	2	Returns the URI for this reference.
Original connector	Type	originalconnectorType	String	2	A string that describes the type of the first reporting connector. This is not the same as the device type.
Original connector	Version	originalconnectorVersion	String	2	The software revision number of the Smartconnector that first reported the event.
Original connector	Zone	originalconnectorZone	Zone	2	The network zone in which the device hosting the first reporting Smartconnector resides.
Original connector	Zone External ID	originalconnectorZoneExternalID	String	2	Returns the external ID for this reference.
Original connector	Zone ID	originalconnectorZoneID	String	2	Returns the ID for the resource in this resource reference.
Original connector	Zone Name	originalconnectorZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original connector	Zone Reference ID	originalconnectorZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and is uniquely identified in the database.
Original connector	Zone Resource	originalconnectorZoneResource	Resource	2	Locates the resource described by this reference.
Original connector	Zone URI	originalconnectorZoneURI	String	2	Returns the URI for this reference.

Request

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Request	Client Application	requestClientApplication	String	2	The client application (such as a web browser) used to issue the request.
Request	Client Application	requestClientApplication	String	2	A description of the client application used to initiate this request, e.g., the HTTP User connector.
Request	Context	requestContext	String	2	A description of the content from which the request originated, e.g., the HTTP Referrer.
Request	Cookies	requestCookies	String	2	Cookie data offered by the client application as part of the request.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Request	Method	requestMethod	String	2	The style of the request, i.e., for an HTTP request this could be PUT or GET.
Request	Protocol	requestProtocol	String	2	The communication protocol used when issuing the request.
Request	URL	requestUrl	String	2	A universal resource locator associated with the event.
Request	URL Authority	requestUrlAuthority	String	2	The URL component used for authentication and authorization.
Request	URL File Name	requestUrlFileName	String	2	The URL component that refers to the file containing the resource.
Request	URL Host	requestUrlHost	String	2	The URL component that specifies the host device where the resource resides.
Request	URL Port	requestUrlPort	Integer	2	The URL component that specifies the port to contact on the host device where the resource resides.
Request	URL Query	requestUrlQuery	String	2	The URL component that specifies the query to use to request the resource.

Source

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Address	sourceAddress	IP address	1	The IP address of the source device.
Source	Asset ID	sourceAssetId	Resource	2	The asset that represents the device that was the network traffic's source.
Source	Asset Name	sourceAssetName	String	2	See the common set of resource attributes.
Source	Asset Resource	sourceAssetResource	Resource	2	See the common set of resource attributes.
Source	DNS Domain	sourceDnsDomain	String	2	The Domain Name Service domain name associated with the user at the source device.
Source	FQDN	sourceFqdn	String	2	The fully qualified domain name associated with the source device. This has no value if either the host name or DNS domain are without a value.
Source	Geo	sourceGeo	GeoDescriptor	1	The geographical information.
Source	Geo Country Code	sourceGeoCountryCode	String	1	Country Code.
Source	Geo Country Flag URL	sourceGeoCountryFlagUrl	String	1	County Flag.
Source	Geo Country Name	sourceGeoCountryName	String	1	Country Code.
Source	Geo Descriptor ID	sourceGeoDescriptorId	ID	1	Unique descriptor for the geo field.
Source	Geo Latitude	sourceGeoLatitude	Double	1	See the common set of geographical attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Geo Location Info	sourceGeoLocationInfo	String	1	See the common set of geographical attributes.
Source	Geo Longitude	sourceGeoLongitude	Double	1	See the common set of geographical attributes.
Source	Geo Postal Code	sourceGeoPostalCode	String	1	See the common set of geographical attributes.
Source	Geo Region Code	sourceGeoRegionCode	String	1	See the common set of geographical attributes.
Source	Host Name	sourceHostName	String	2	The name of the source device.
Source	MAC Address	sourceMacAddress	MAC address	2	The MAC address associated with the network traffic's source (which may or may not be the MAC address of the host device).
Source	NT Domain	sourceNtDomain	String	2	The Windows NT domain associated with the source device.
Source	Port	sourcePort	Integer	1	The network port associated with the network traffic's source.
Source	Process Name	sourceProcessName	String	2	The name of the process associated with the source of the network traffic.
Source	Service Name	sourceServiceName	String	2	The name of the service associated with the network traffic's source.
Source	Translated Address	sourceTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device that was the network traffic's source.
Source	Translated Port	sourceTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Translated Zone	sourceTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device that was the network traffic's source.
Source	Translated Zone External ID	sourceTranslatedZoneExternalID	String	1	Returns the external ID for this reference.
Source	Translated Zone ID	sourceTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Source	Translated Zone Name	sourceTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Source	Translated Zone Reference ID	sourceTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Source	Translated Zone Resource	sourceTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
Source	Translated Zone URI	sourceTranslatedZoneURI	String	1	Returns the URI for this reference.
Source	User ID	sourceUserId	String	2	The OS- or application-based identifier associated with the user at the network traffic's source.
Source	User Name	sourceUserName	String	2	The OS- or application-based name associated with the user at the network traffic's source.
Source	User Privileges	sourceUserPrivileges	String	2	The privileges afforded the user at the network traffic's source.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Zone	sourceZone	Zone	1	The network zone where the source device resides.
Source	Zone External ID	sourceZoneExternalID	String	1	Returns the external ID for this reference.
Source	Zone ID	sourceZoneID	String	1	Returns the ID for the resource in this resource reference.
Source	Zone Name	sourceZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Source	Zone Reference ID	sourceZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Source	Zone Resource	sourceZoneResource	Resource	1	Locates the resource described by this reference.
Source	Zone URI	sourceZoneURI	String	1	Returns the URI for this reference.

Target

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Address	targetAddress	IP address	1	The IP address of the device hosting the attacker.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Asset ID	targetAssetId	Resource	2	The asset that represents the attacked device's host.
Target	Asset Name	targetAssetName	String	2	See the common set of resource attributes.
Target	Asset Resource	targetAssetResource	Resource	2	See the common set of resource attributes.
Target	DNS Domain	targetDnsDomain	String	2	The Domain Name Service domain name associated with the attacked device.
Target	FQDN	targetFqdn	String	2	The fully qualified domain name associated with the attacked device.
Target	Geo	targetGeo	GeoDescriptor	1	The geographical information.
Target	Geo Country Code	targetGeoCountryCode	String	1	Country code.
Target	Geo Country Flag URL	targetGeoCountryFlagUrl	String	1	County flag.
Target	Geo Country Name	targetGeoCountryName	String	1	Country name.
Target	Geo Descriptor ID	targetGeoDescriptorId	ID	1	Unique descriptor for the geo field.
Target	Geo Latitude	targetGeoLatitude	Double	1	Latitude.
Target	Geo Location Info	targetGeoLocationInfo	String	1	Location information.
Target	Geo Longitude	targetGeoLongitude	Double	1	Longitude.
Target	Geo Postal Code	targetGeoPostalCode	String	1	Postal code.
Target	Geo Region Code	targetGeoRegionCode	String	1	Region code.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Host Name	targetHostName	String	2	The name of the attacked device.
Target	MAC Address	targetMacAddress	MAC address	2	The MAC address associated with the target of the attack (which may or may not be the MAC address of the host device).
Target	NT Domain	targetNtDomain	String	2	The Windows NT domain associated with the attacked device.
Target	Port	targetPort	Integer	1	The network port associated with the target of the attack.
Target	Process Name	targetProcessName	String	2	The name of the process associated with the attack's target.
Target	Service Name	targetServiceName	String	2	The name of service associated with the attack's target.
Target	Translated Address	targetTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the attacked device.
Target	Translated Port	targetTranslatedPort	Integer	1	If network address translation is an issue, this is the translated port associated with the attack.
Target	Translated Zone	targetTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the targeted device.
Target	Translated Zone External ID	targetTranslatedZoneExternalID	String	1	Returns the external ID for this reference.
Target	Translated Zone ID	targetTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Translated Zone Name	targetTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Target	Translated Zone Reference ID	targetTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Target	Translated Zone Resource	targetTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
Target	Translated Zone URI	targetTranslatedZoneURI	String	1	Returns the URI for this reference.
Target	User ID	targetUserId	String	2	The OS- or application-based identifier associated with the attacker, at the target of the attack.
Target	User Name	targetUserName	String	2	The OS- or application-based name associated with the attacker, at the target of the attack.
Target	User Privileges	targetUserPrivileges	String	2	The privileges afforded the attacker, at the target of the attack.
Target	Zone	targetZone	Zone	1	The network zone in which the attacked device resides.
Target	Zone External ID	targetZoneExternalID	String	1	Returns the external ID for this reference.
Target	Zone ID	targetZoneID	String	1	Returns the ID for the resource in this resource reference.
Target	Zone Name	targetZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Zone Reference ID	targetZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Target	Zone Resource	targetZoneResource	Resource	1	Locates the resource described by this reference.
Target	Zone URI	targetZoneURI	String	1	Returns the URI for this reference.

Threat

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Threat	Asset Criticality	assetCriticality	Integer	2	The relative measure of the importance of the targeted device, on a scale of 0 to 10.
Threat	Model Confidence	modelConfidence	Integer	2	The relative measure of ArcSight's confidence in its model of the attacked device, on a scale of 0 to 10.
Threat	Priority	priority	Integer	1	The relative measure of importance of investigating this event on a scale of 0 to 10. This field incorporates Model Confidence.
Threat	Relevance	relevance	Integer	2	The relative measure of likelihood that this event succeeded, on a scale of 0 to 10.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Threat	Severity	severity	Integer	2	The relative measure of possible damage to network security represented by the event on a scale of 0 to 10. It may be noted that **event severity** is supplied by the device; **ArcSight severity** is supplied by the Smartconnector; and **attack severity** is supplied by the threat evaluation process.

Resource Attributes

Attribute Suffix	Description
External ID	The user-defined identifier associated with a configuration resource.
ID	The internal identifier associated with a resource (a UUID).
Reference ID	The internal identifier associated with the resource reference (an integer).
Type Name	The type of configuration resource.
URI	The URI associated with the resource (e.g., /All Users/Administrators/Mlow).

Geographical Attributes

Attribute Suffix	Description
Descriptor ID	The internal ID of the geographical reference.
Country Code	The identifier for the national-political state in which a device resides.
Country Flag URL	The URL of an image of the flag of the national-political state in which the device resides.
Country Name	The name of the national-political state where a device resides.
Latitude	The latitude of a device (Float).
Location Info	Other, free-form text information about the device's location.
Longitude	The longitude of a device (Float).

Attribute Suffix	Description
Postal Code	The postal code of the device's location, as assigned by the national-political state where it resides.
Region Code	The identifier of the sub-region of the national-political state where a device resides. The style of the identifier varies with the host country.

Audit Events

Audit events are ones generated within ArcSight itself to mark a wide variety of routine actions that can occur manually or automatically, such as adding an event to a case or when a Moving Average data monitor detects a rapidly rising moving average. Audit events have many applications, which can include notifications, task validation, compliance tracking, automated housekeeping, and system administration.

In the table below, use the **Audit Event Category** to locate events. The **Audit Event Description** approximates the Name you see in active channel grids. Additional details, when necessary, appear in the Notes column.

Compare audit events, which report on system activity, with Status Monitor Events, which provide information about a wide variety of system states.

Audit Event Categories

- Active Channel
- Active List
- Agent Connection
- Agent Exceptions
- Agent Login
- Agent Registration and Configuration
- Authorization
- Configuration Resources
- Dashboard
- Manager Activation
- Manager Database Error Conditions
- Manager External Event Flow Interruption
- Moving Average Data Monitor
- Notification
- Notification Acknowledgement
- Notification Testing
- Partition Archiver
- Partition Manager
- Reconciliation Data Monitor
- Report
- Resource Quota
- Rule Actions

- Rule Activations
- Rule Firings
- Rule Warnings
- Scheduler Execution
- Scheduler Scheduling Tasks
- Scheduler Skip
- Statistical Data Monitor
- Stress
- User Login

ArcSight Audit Events

Audit Event Category	Device Event Class ID	Audit Event Description
Active Channel	activechannel:100	An active channel was opened
Active Channel	activechannel:101	An empty active channel was opened
Active List	activelist:101	An entry was added to an active list
Active List	activelist:102	An entry was removed from an active list
Active List	activelist:103	An entry was changed in an active list
Agent Connection	agent:009	Manager rejected a connection attempt from an agent for reasons other than authentication failure
Agent Connection	agent:30	Agent started
Agent Connection	agent:31	Agent shutdown
Agent Connection	agent:101	Agent has just connected to Manager
Agent Connection	agent:102	Agent is sending events but no heartbeats
Agent Connection	agent:103	Agent is sending neither events nor heartbeats
Agent Connection	agent:104	An unknown agent attempted to connect to the Manager
Agent Connection	agent:105	An agent presented an incorrect shared secret when authenticating
Agent Exceptions	agent:012	Agent detected source events from a sensor device containing incorrect time stamps
Agent Exceptions	agent:013	Agent noted that a new sensor device is sending events
Agent Exceptions	agent:014	Agent could not find a base event referenced in a syslog aggregate event
Agent Exceptions	agent:016	Agent successfully connected to the sensor device's log
Agent Exceptions	agent:017	Agent successfully executed a command
Agent Exceptions	agent:018	Agent could not execute a command
Agent Exceptions	agent:019	Agent is caching events because they could not be immediately transmitted to the Manager

Audit Event Category	Device Event Class ID	Audit Event Description
Agent Exceptions	agent:020	Agent has emptied its cache of events
Agent Exceptions	agent:021	Agent could not communicate with an NT collector sensor
Agent Exceptions	agent:023	Agent could not communicate with a CheckPoint sensor
Agent Exceptions	agent:024	Agent is having difficulty communicating with CheckPoint
Agent Exceptions	agent:028	Agent experienced an unexpected problem
Agent Exceptions	agent:029	Agent was forced to drop its cached data
Agent Exceptions	agent:030	Agent cache filled and part of the cached data was deleted
Agent Login	authentication:200	Successful Agent authentication
Agent Login	authentication:201	Agent authentication failed
Agent Registration and Configuration	agent:007	Agent successfully registered with Manager
Agent Registration and Configuration	agent:008	Agent did not successfully register with Manager
Agent Registration and Configuration	agent:029	Agent configuration was successfully changed
Agent Registration and Configuration	agent:022	Agent could not process a reconfiguration request
Agent Registration and Configuration	agent:032	Agent configuration was successfully changed
Agent Registration and Configuration	agent:025	Agent content was successfully updated
Agent Registration and Configuration	agent:026	Agent content update failed
Agent Registration and Configuration	agent:010	Agent upgrade succeeded, This is currently in the context of an installer upgrade.
Agent Registration and Configuration	agent:011	Agent upgrade failed. This event is not currently being generated.
Authorization	authorization:100	Manager refused to authorize client
Configuration Resources	resource:100	Deleted a configuration resource
Configuration Resources	resource:101	Updated a configuration resource
Configuration Resources	resource:102	Added a new configuration resource
Configuration Resources	resourcereference:100	Could not locate a configuration resource. Through the supplied universal resource identifer (URI).
Dashboard	dashboard:100	Dashboard has opened

Audit Event Category	Device Event Class ID	Audit Event Description
Manager Activation	manager:100	Manager has started
Manager Activation	manager:101	A clean Manager shutdown has been requested
Manager Database Error Conditions	database:100	Database tablespace is low and will be deactivated
Manager Database Error Conditions	database:101	Database has generated a fatal error and will be deactivated
Manager Database Error Conditions	database:102	Database has been reactivated
Manager Database Error Conditions	database:103	Database has more tablespace available after detecting a low tablespace condition
Manager External Event Flow Interruption	manager:200	Manager has stopped the event flow
Manager External Event Flow Interruption	manager:201	Manager has allowed the event flow to resume
Moving Average Data Monitor	datamonitor:102	Moving Average data monitor detected a rapidly falling moving average
Moving Average Data Monitor	datamonitor:103	Moving Average data monitor detected a rapidly rising moving average
Moving Average Data Monitor	datamonitor:104	Moving Average data monitor reporting the current moving average
Notification	notification:100	Notification has been disabled
Notification	notification:101	Notification has been disabled because the queue of notifications to be sent is too large
Notification	notification:102	Notification has been enabled
Notification	notification:103	Notification has been enabled because the queue of notifications is back under control
Notification	notification:104	A particular notification destination has been disabled
Notification	notification:105	A particular notification destination has been disabled because too much traffic was directed at it
Notification	notification:106	A particular notification destination has been enabled
Notification	notification:107	A notification expired without being acknowledged
Notification	notification:108	A functioning destination could not be located for this notification
Notification	notification:109	Old notification has been purged
Notification Acknowledgement	notification:300	This notification has been acknowledged
Notification Testing	notification:200	Sent a test notification to this destination group

Audit Event Category	Device Event Class ID	Audit Event Description
Partition Archiver	partitionarchiver:100	The partition was successfully archived
Partition Archiver	partitionarchiver:200	There was a problem while archiving the partition
Partition Archiver	partitionarchiver:300	Partition archiving is disabled
Partition Archiver	partitionarchiver:400	Partition archiving did not complete in the alotted time
Partition Archiver	partitionarchiver:500	Partition archiving failed
Partition Archiver	partitionarchiver:600	There was an unexpected error while archiving partitions
Partition Manager	partitionmanager:100	Partitions have been successfully rotated
Partition Manager	partitionmanager:200	There was a problem rotating partitions
Partition Manager	partitionmanager:300	The partition manager has been disabled
Partition Manager	partitionmanager:500	Partitions could not be rotated
Partition Manager	partitionmanager:600	There was an unexpected error while rotating partitions
Reconciliation Data Monitor	datamonitor:300	Correlation data monitor reporting a correlated or non-correlated event
Report	report:100	Generated a new archived-report configuration resource
Report	report:101	Failed to generate a new archived-report configuration resource
Report	report:102	Generated a new delta archived-report configuration resource
Resource Quota	quota:100	Resource usage has fallen below the fixed-quota level
Resource Quota	quota:101	Resource usage has exceeded the fixed-quota level
Resource Quota	quota:102	Asset autocreation has exceeded a fixed quota
Resource Quota	quota:103	Asset autocreation is proceeding too rapidly
Rule Actions	rule:301	Set Severity action. This event has been deprecated.
Rule Actions	rule:302	Set Event Attribute action
Rule Actions	rule:303	Send to Notifier action
Rule Actions	rule:304	Execute Command action
Rule Actions	rule:305	Export... action
Rule Actions	rule:306	Create New Case action
Rule Actions	rule:307	Add to Case action

Audit Event Category	Device Event Class ID	Audit Event Description
Rule Actions	rule:308	Create New Case action failed
Rule Actions	rule:309	Add to Case action failed
Rule Actions	rule:310	Add to Active List action
Rule Actions	rule:311	Move between Active Lists action. This event has been deprecated.
Rule Actions	rule:312	Remove from Active List action
Rule Activations	rule:700	Rule has been deactivated
Rule Activations	rule:701	Rule has been deactivated because it is unsafe. There was excessive recursion or event matching.
Rule Activations	rule:702	Rule has been activated
Rule Firings	rule:101	Rule fired OnEveryEvent
Rule Firings	rule:102	Rule fired OnFirstEvent
Rule Firings	rule:103	Rule fired OnSubsequentEvents
Rule Firings	rule:104	Rule fired OnEveryThreshold
Rule Firings	rule:105	Rule fired OnFirstThreshold
Rule Firings	rule:106	Rule fired OnSubsequentThresholds
Rule Firings	rule:107	Rule fired OnTimeUnitExpiration
Rule Warnings	rule:501	Rule is firing on events generated by itself
Scheduler Execution	scheduler:200	A task has been executed
Scheduler Execution	scheduler:201	A task failed to execute
Scheduler Scheduling Tasks	scheduler:300	A new task has been scheduled
Scheduler Scheduling Tasks	scheduler:301	A new task could not be scheduled
Scheduler Scheduling Tasks	scheduler:302	Enabled a task
Scheduler Scheduling Tasks	scheduler:303	Could not enable a task
Scheduler Scheduling Tasks	scheduler:304	Deleted a task
Scheduler Scheduling Tasks	scheduler:305	Failed to delete a task
Scheduler Scheduling Tasks	scheduler:306	Disable a task
Scheduler Scheduling Tasks	scheduler:307	Could not disable a task

Audit Event Category	Device Event Class ID	Audit Event Description
Scheduler Skip	scheduler:100	The task scheduler skipped a scheduled task execution because the scheduler was not allowed to run
Scheduler Skip	scheduler:101	The task scheduler skipped a scheduled task invocation because the last invocation of the task is still executing
Statistical Data Monitor	datamonitor:200	Statistical Data Monitor reporting a change in status
Stress	test:100	A stress test event. This event is generated only by ArcSight Quality Assurance.
User Login	authentication:100	Successful client login
User Login	authentication:101	Failed client login
User Login	authentication:102	Client logout
User Login	authentication:103	Client timed out due to inactivity
User Login	authentication:104	Too many client login failures occurred within a time period

Status Monitor Events

ArcSight status monitor events can reveal and isolate many different quantity and time-unit issues that bear directly on performance and capacity. There are many possible applications of this system-state data, but those applications must always be interpreted within the context of your particular hardware, software, and network environment, and the deployment choices made for ArcSight and its SmartConnectors.

Compare status monitoring events, which provide information about a wide variety of system states, to Audit Events, which report on system activity.

- Active Channel Statistics
- Active List Statistics
- Asset Statistics
- Data Monitor Statistics
- Event Broker Statistics
- Filter Engine Statistics
- Main Flow Statistics
- Notification Statistics
- Pattern Discovery Statistics
- Report Statistics
- Resource Framework Statistics
- Rules Engine Statistics
- Session Management Statistics
- Side Table Statistics
- SmartConnector Flow Statistics

Active Channel Statistics

Active channel statistics, specifically any changes that occur in the counts they report, can indicate performance issues and the use of processing cycles. These events summarize:

- The number of events changed across all open Active Channels per second
- The number of events inserted into Active Channels per second
- The number of currently open Active Channels

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/ActiveChannels/Open	monitor:100	Open active channel count. Provides count and current value.
/Monitor/ActiveChannels/Events/Insertions	monitor:174	Active channel event insertions per second. Provides count per second since last monitor event.
/Monitor/ActiveChannels/Events/Changes	monitor:175	Active channel event changes per second. Provides count per second since last monitor event.

Active List Statistics

Active list statistics monitor the resources being used by active lists. Active lists entries use some memory and database resources, and use CPU resources when they are referenced by other parts of the system (e.g., rules, reports, and filters). While changes to these temporary lists are not persisted, they do represent some memory overhead. Note that when active lists are used by replay-with-rules, this also creates temporary lists.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/ActiveLists/ListCount	monitor:114	Open active list count. Provides count, current value.
/Monitor/ActiveLists/EntryCount	monitor:115	Active list entry count. Provides count, current value.
/Monitor/ActiveLists/EntryCapacity	monitor:116	Active list entry capacity. Provides count, current value.
/Monitor/ActiveLists/EntryPercentUsed	monitor:117	Active list entry usage. Provides percent, current value.
/Monitor/ActiveLists/TemporaryListCount	monitor:118	Temporary Active list count. Provides count, current value.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/ActiveLists/TemporaryEntryCount	monitor:119	Temporary Active list entry count. Provides count, current value.
/Monitor/ActiveLists/TemporaryCapacity	monitor:120	Temporary Active list capacity. Provides count, current value.
/Monitor/ActiveLists/TemporaryPercentageUsed	monitor:121	Temporary Active list usage. Provides percent, current value.
/Monitor/ActiveLists/QueriesPerSecond	monitor:122	Active list queries per second. Provides count of queries per second since startup.
/Monitor/ActiveLists/ChangesPerSecond	monitor:123	Active list changes per second. Count per second since startup.

Asset Statistics

Asset statistics offer insight into performance areas that affect assets in the system and can help resolve source, destination, agent, and device asset issues for incoming events. These events summarize:

- **Asset resolutions per second** is the average number of end-points in events, that are resolved to assets in a second.
- **Asset resolutions average time** is the average time in milliseconds taken to resolve an end-point in an event to an asset.
- **Asset scanner events per second** is the number of scanner events processed in a second.
- Asset scanner events average time is the average time in milliseconds taken to process a scanner event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Asset/TotalCount	monitor:200	Asset total count. Provides count, current value.
/Monitor/Asset/Scanner/EventsPerSecond	monitor:201	Scanner events processed per second. Provides count per second since last monitor event.
/Monitor/Asset/ResolutionsPerSecond	monitor:202	Asset resolutions per second. Provides count per second for asset resolutions since last monitor event.
/Monitor/Asset/Scanner/AverageTime	monitor:203	Scanner event average processing time. Provides count per second for scanner event average processing time since starup.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Asset/ResolutionsAverageTime	monitor:204	Asset resolution average time. Provides average time in milliseconds for asset resolution since startup.
/Monitor/Asset/ResolutionsAverageTime/Source	monitor:205	Asset source resolution average time. Provides average time in milliseconds for asset source resolution since startup.
/Monitor/Asset/ResolutionsAverageTime/Destination	monitor:206	Asset destination resolution average time. Provides average time in milliseconds for asset destination resolution since startup.
/Monitor/Asset/Size	monitor:240	Transitive Closure Size. Provides count per second and current value for transitive closure size.

Data Monitor Statistics

The data monitor statistics indicate how intensively the data monitors are working, which in turn can indicate situations such as filters needing adjustment or data monitors needing restructuring. These events summarize:

- **Active probes** is the number of currently enabled data monitors.
- **Evaluations per second** is the number of events times the number of enabled data monitors per second.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/DataMonitors/ActiveProbes	monitor:101	Active data monitor probe count. Provides count, current value.
/Monitor/DataMonitors/EvaluationsPerSecond	monitor:124	Data monitor evaluations per second. Provides count per second since last monitor event.

Event Broker Statistics

These statistics monitor reading events from, and writing events to, the database. As such, they are database health indicators. These events summarize:

- **Event count** is the number of events inserted into the database since the last monitor event.
- **Insert time** is the average time taken to insert each event into the database, in microseconds.

- **Retrieval time** is the average time taken to retrieve each event from the database in microseconds.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/EventBroker/InsertTime	monitor:102	Events insertion time per event Provices count in microseconds for insertion time per event since last monitor event.
/Monitor/EventBroker/InsertedEventCount	monitor:103	Events processed count. Provides count since last monitor event.
/Monitor/EventBroker/RetrievalTime	monitor:140	Events retrieval time per event. Provides count in microseconds per count, since last monitor event.

Filter Engine Statistics

The count of in-memory filter evaluations can serve as a broad indicator of filter performance.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Filters/EvaluationCount	monitor:161	Filter evaluation count.

Main Flow Statistics

These events report statistically on the overall throughput of the ArcSight Manager, for both incoming and internal events. This flow is the sequence of processing steps applied to each event and is a broad indicator or benchmark of system traffic. These events summarize:

- **Count** describes the number of events that have passed through the flow since the manager started.
- **Rate** describes the current event rate in events per second.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/MainFlow/EPS	monitor:230	Main flow event rate. Provides count per second since last monitor event.
/Monitor/MainFlow/Events	monitor:231	Main flow event count. Provides count since startup.

Notification Statistics

This group reports on notification activity, which can be of diagnostic value in detecting unusually high notifications activity.

- **New count** describes the number of new notifications since the last monitor event.

- **Escalated count** describes the number of notifications that were escalated since the last monitor event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Notification/New	monitor:180	New notification count. Provides count since last monitor event.
/Monitor/Notification/Escalated	monitor:181	Escalated notification count. Provides count since last monitor event.

Pattern Discovery Statistics

These events provide statistics for recent or pending pattern discovery runs. Because pattern discovery is database-intensive, these statistics can indicate or help diagnose database performance issues.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Patterns/RunCount	monitor:190	Pattern discoveries run count. Provides count since last monitor event.
/Monitor/Patterns/RunsQueued	monitor:191	Pattern discoveries queued count. Provides count current value.

Report Statistics

These events provide statistics about the current number of reports querying the database or being rendered. Because reports are database-intensive, these statistics can indicate or help diagnose database performance issues.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Reports/Running	monitor:130	Reports running count. Provides count, current value.
/Monitor/Reports/RunningQueryingDB	monitor:131	Reports querying database count. Provides count, current value.
/Monitor/Reports/RunningRendering	monitor:132	Reports rendering count. Provides count, current value.

Resource Framework Statistics

Resource-framework events report on the database activity connected with updates (reads, writes, and deletions) to system resources such as rules, assets, and filters, since the last

monitor event. This data can be valuable in tracking or diagnosing performance-related issues such as automatic asset maintenance, the threat-level formula, or rule-driven usage.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Resource/Activity/Insert	monitor:171	Resources inserted per second. Provides count per second since last monitor event.
/Monitor/Resource/Activity/Update	monitor:172	Resources updated per second. Provides count per second since last monitor event.
/Monitor/Resource/Activity/Delete	monitor:173	Resources deleted per second. Provides count per second since last monitor event.

Rules Engine Statistics

The statistics related to the ArcSight Manager's rules engine can help reveal performance issues in several areas. Please remember that information about rules activity always needs to be considered in the full content of the Manager's operations. For example, a busy Moving Average data monitor, if used inefficiently, can affect several of these statistics; a poorly written rule can inadvertently drive up the rate of actions executed.

These statistics have the following performance implications

- Count of events inserted into the rule engine: CPU.
- Rate of event insertion into the rule engine: CPU.
- Count of correlated events generated by the rule engine: CPU.
- Rate of correlated event generation by the rule engine: CPU.
- Count of partial matches in the rule engine: memory.
- Count of events that are still present in rule engine's working memory: memory.
- Count of groupBy cells that are being used by the rule engine: memory.
- Count of rules currently active in the rule engine: comparative value only.
- Rate of actions being executed by the rule engine: CPU.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Rules/InsertedEventCount	monitor:151	Rules total event count. Provides count since last monitor event.
/Monitor/Rules/InsertedEventRate	monitor:152	Rules inserted events per second. Provides count per second since last monitor event.
/Monitor/Rules/GeneratedEventRate	monitor:153	Rules generated events per second. Provides count per second since last monitor event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Rules/PartialMatchCount	monitor:154	Rules partial match count. Provides count, current value.
/Monitor/Rules/EventsInRuleEngineMemory	monitor:155	Rules in-memory event count. Provides count, current value.
/Monitor/Rules/GroupByCellsSize	monitor:156	Rules group by cells size. Provides count, current value.
/Monitor/Rules/ActiveRulesCount	monitor:157	Active rules count. Provides count, current value.
/Monitor/Rules/ActionsTakenRate	monitor:158	Rules actions rate. Provides count per second since last monitor event.
/Monitor/Rules/GeneratedEventCount	monitor:159	Rules generated event count. Provides count since last monitor event.

Session Management Statistics

This statistic tracks the current number of active user sessions.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Sessions/Active/Total	monitor:160	Active session count. Provides count and current value.

Side Table Statistics

Side tables are ones held in-memory and in the database to retain common and relatively static information, similar to a cache. The purpose is to improve access times for inserts and queries. Side tables store event data that includes: geographical information, categorization information, agent information, device information and labels for custom strings and numbers.

- **Size** identifies how many entries are presently in the cache.
- **Insert** identifies the number of inserts in the past two hours.
- **Cache** misses identifies how many failed attempts to find entries occurred in the past two hours.

- **Cache hit rate** identifies how many successful attempts to find entries occurred in the past two hours.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/SideTable/GeoInfo/HitRate	monitor:210	Geo info sidetable cache hit rate. Provides a percentage over a moving time frame.
/Monitor/SideTable/GeoInfo/Inserts	monitor:211	Geo info sidetable inserts. Provides count over a moving timeframe.
/Monitor/SideTable/GeoInfo/CacheMisses	monitor:212	Geo info sidetable cache misses. Provides count over a moving timeframe.
/Monitor/SideTable/GeoInfo/Size	monitor:213	Geo info sidetable size. Provides count, current value.
/Monitor/SideTable/Category/HitRate	monitor:214	Category sidetable cache hit rate. Provides a percentage over a moving timeframe.
/Monitor/SideTable/Category/Inserts	monitor:215	Category sidetable inserts. Provides count over a moving timeframe.
/Monitor/SideTable/Category/CacheMisses	monitor:216	Category sidetable cache misses. Provides count over a moving timeframe.
/Monitor/SideTable/Category/Size	monitor:217	Category sidetable size. Provides count, current value.
/Monitor/SideTable/Agent/HitRate	monitor:218	Agent sidetable cache hit rate. Provides a percentage over a moving timeframe.
/Monitor/SideTable/Agent/Inserts	monitor:219	Agent sidetable inserts. Provides count over a moving timeframe.
/Monitor/SideTable/Agent/CacheMisses	monitor:220	Agent sidetable cache misses. Provides count over a moving timeframe.
/Monitor/SideTable/Agent/Size	monitor:221	Agent sidetable size. Provides count, current value.
/Monitor/SideTable/Device/HitRate	monitor:222	Device sidetable cache hit rate. Provides a percentage over a moving timeframe.
/Monitor/SideTable/Device/Inserts	monitor:223	Device sidetable inserts. Provides count over a moving timeframe.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/SideTable/Device/CacheMisses	monitor:224	Device sidetable cache misses. Provides count over a moving timeframe.
/Monitor/SideTable/Device/Size	monitor:225	Device sidetable size. Provides count, current value.
/Monitor/SideTable/Labels/HitRate	monitor:226	Labels sidetable cache hit rate. Provides a percentage over a moving timeframe.
/Monitor/SideTable/Labels/Inserts	monitor:227	Labels sidetable inserts. Provides count over a moving timeframe.
/Monitor/SideTable/Labels/CacheMisses	monitor:228	Labels sidetable cache misses. Provides count over a moving timeframe.
/Monitor/SideTable/Labels/Size	monitor:229	Labels sidetable size. Provides count, current value.

SmartConnector Flow Statistics

SmartConnector flow statistics record the event rates that occur at different stages of agent processing. "Sum of" statistics are sums of all values reported by all agents connected to the ArcSight Manager. All values are statistics over the past 1-minute range. These events summarize:

- **Received event rate** is the rate at which agents receive events from devices.
- Post filter event rate is the rate of events that passed the filter (e.g., were not filtered out).
- **Post aggregation event rate** is the rate of event aggregation.
- **Agent-to-manager event rate and count** describe how many events were actually sent to the Manager.
- **Cache size** describes the estimated size of the on-disk agent event cache.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Agents/Events/ToManager	monitor:104	Agent output event count, since startup. Provides count.
/Monitor/Agents/EPS/ToManager	monitor:109	Agent output event rate. Provides count per second and agent-to-manager since last monitor event.
/Monitor/Agents/EPS/Received	monitor:110	Agent input event rate. Provides count per second for the agent received event rate since last monitor event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description
/Monitor/Agents/EPS/PostFilter	monitor:111	Agent filtered event rate. Provides count per second for the agent post-filter event rate since last monitor event.
/Monitor/Agents/EPS/PostAggregation	monitor:112	Agent aggregated event rate. Provides count per second for the agent post-aggregation event rate since last monitor event.
/Monitor/Agents/CacheSize	monitor:113	Estimated agent cache size, current value. Provides count.
/Monitor/Agents/Total/Events/ToManager	monitor:141	Sum of agent output event counts. Provides count-per-second sum of agent-to-manager event counts since startup.
/Monitor/Agents/Total/EPS/ToManager	monitor:146	Sum of agent-to-manager output event rates. Provides counted per-second since last monitor event.
/Monitor/Agents/Total/EPS/Received	monitor:147	Sum of agent input event rates. Provides count per second for the sum of agent received event rates since last monitor event.
/Monitor/Agents/Total/EPS/PostFilter	monitor:148	Sum of agent filtered event rates. Provides count per second for the sum of agent post-filter event rates since last monitor event.
/Monitor/Agents/Total/EPS/PostAggregation	monitor:149	Sum of agent aggregated event rates. Provides count per second for the sum of agent post-aggregation event rates since the last monitor event.
/Monitor/Agents/Total/CacheSize	monitor:150	Sum of estimated agent cache sizes. Provides count as a sum of the estimated agent cache sizes current value.

Chapter 5

Using Cases

ArcSight cases provide organized, workflow-style tracking and management of interesting events or situations.

The ArcSight Web interface enables you to create, manage, or customize cases.

Cases have a large number of fields to cover a wide range of event analysis and investigation possibilities. (See “Creating Cases” on page 95.).

You can add an **Export** button to the Cases display to export selected cases. Add the line `ui.export.enabled=true` to the `webserver.properties` file and restart ArcSight Web.

“Managing Cases” on page 93

“Creating Cases” on page 95

Managing Cases

The cases display shows cases that are already created in the Cases tree. From the main panel, you can select, view, and customize existing cases, and create new ones.

To view an existing case

1. Navigate to and select the case in the Cases resource tree on the left.
   - Click the group folders in the tree to open or close them.
   - Click a folder to see a list of its cases in the pane to the right.
   - Click the arrow icon in the upper-right corner of the resource pane to hide it or show it.
2. The Cases content pane shows individual listings. Click an individual case to see its fields (see “Creating Cases” on page 95).

To edit an individual case

1. Click **Lock this case**.
2. Make your changes and click **Submit**.
3. Unlock a case after you finish editing.

To remove a case

1. Select the check box for the case you want to remove and click **Remove**.

If you want to keep the case but not allow others to edit it, you can Lock (hold for editing) or Unlock (release for others to edit) buttons.

2 Click **Refresh** to update the display.

To create a new case

Click **New Case** to go to the Create a New Case display. For details about how to create a case, see "Creating Cases" on page 95.

To customize a case

Click **Customize** to select, deselect, and arrange the columns of the case list.

Default Case Management Columns

Attribute	Description
Name	The name assigned to the case. Using descriptive names is important.
Locked	Whether the case is free to be edited by others. If Locked, it cannot.
Security Classification Code	The letter codes that identify the nature of the security issues the case represents. See "Security Classification Default Letter Codes" on page 94 below.
Ticket Type	The source of the case or its means of tracking.
Stage	The current collaboration or workflow stage assigned to the case.
Frequency	The numerical range of events that occur in regard to a case.
Created By	The ArcSight user ID of the person who created the case.

Security Classification Default Letter Codes

Classification Category	Letter Codes
Attack Mechanism	I = Informational
	O = Operational
	P = Physical
	U = Unknown
Attack Agent	C = Collaborative
	I = Insider
	O = Outsider
	U = Unknown
Vulnerability	D = Design
	E = Operational Environment
	O = Operational
	U = Unknown

Classification Category	Letter Codes
Sensitivity	C = Confidential
	S = Secret
	T = Top Secret
	U = Unclassified
Associated Impact	A = Availability
	C = Confidentiality
	I = Integrity
	U = Unknown
Action	B = Block/Shutdown
	M = Monitoring
	O = Other

Creating Cases

To create a case, choose the Initial attributes tab first. Fill in the required and other appropriate fields, tab by tab, then click **Submit** at the bottom of the display. Overall, the tabs represent:

- **Initial** - Basic case information: case ticket attributes, description and security classification.
- **Follow Up** - Description of actions taken, planned, or recommended.
- **Final** - Ticket resolution and reporting including attack mechanism, attack agent, incident information, and vulnerability information.
- **Events** - List of events included in case.
- **Notes** - Miscellaneous information applicable to a case.

Display ID numbers are assigned automatically when you save the case.

Initial Tab

The fields on this tab provide basic case information.

Field		Description
Case		
	Name	Required field specifying name of case.
	Display ID	An automatically assigned unique number.
Ticket		
	Ticket Type	Drop-down list includes Internal, Client, and Incident types.

Field		Description
	Stage	Indicate workflow stage of ticket; selections include Queued, Initial, Follow-up, Final, and Closed.
	Frequency	Indicates how often reported issue occurs. Values assigned are 0 (never or once), 1 (less than 10 times), 2 (10 to 15 times), 3 (15 times), 4 (more than 15).
	Operational Impact	Impact of reported issue. Values assigned are 0 (no impact), 1 (no immediate impact), 2 (low-priority impact), 3 (high-priority impact), 4 (immediate impact).
	Security Classification	Values assigned are 1 (Unclassified), 2 (Confidential), 3 (Secret), 4 (Top Secret).
	Consequence Severity	Values assigned are 0 (None), 1 (Insignificant), 2 (Marginal), 3 (Critical), 4 (Catastrophic).
	Reporting Level	This is a calculated number, based on Ticket info values entered.
Incident Information		
	Detection Time	This field is auto-populated.
	Estimated Start Time	This field is auto-populated.
	Estimated Restore Time	This field is auto-populated.
	External ID	This field is auto-populated.
	Alias	Another name by which the incident is referenced in the system.
	Description	A text description of the incident.
Assign		
	Owner	Users designated as owners of the case.
	Notification Groups	Pre-defined groups that should be notified when the case is created or updated.
Description		
	Affected Services	This text field can contain up to 4,000 characters.
	Affected Elements	This text field can contain up to 4,000 characters.
	Estimated Impact	This text field can contain up to 4,000 characters.
	Affected Sites	This text field can contain up to 4,000 characters.
Security Classification		

Field		Description
	Attack Mechanism	I = Informational O = Operational P = Physical U = Unknown
	Attack Agent	C = Collaborative I = Insider O = Outsider U = Unknown
	Incident Source 1	This field is auto-populated.
	Incident Source 2	This field is auto-populated.
	Vulnerability	D = Design E = Operational Environment U = Unknown
	Sensitivity	C = Confidential S = Secret T = Top Secret U = Unclassified
	Associated Impact	A = Availability C = Confidentiality I = Integrity U = Unknown
	Action	B = Block/Shutdown M = Monitoring O = Other
Security Classification Code		
	Security Classification Code	This field is auto-populated.

Follow Up Tab

The fields on this tab describe follow-up entries for a case.

Field	Description
Actions Taken	This text field can contain up to 4,000 characters.
Planned Actions	This text field can contain up to 4,000 characters.
Recommended Actions	This text field can contain up to 4,000 characters.
Follow-up Contact	This text field can contain up to 4,000 characters.

Final Tab

Fields on this tab provide ticket resolution and reporting information related to the attack agent associated with a case.

Field		Description
Attack Mechanism		
	Attack Mechanism	This field is auto-populated.
	Attack Protocol	The network protocol that is transporting the attack.
	Attack OS	The operating system supporting the attack.
	Attack Program	The program that is performing the attack.
	Attack Time	The date and time of the attack.
	Attack Target	The host or device at which the attack is directed.
	Attack Service	The service at which the attack is directed.
	Attack Impact	The effect of the attack.
	Final Report Action	The action recommended for this case.
Attack Agent		
	Attack Agent	This field is auto-populated.
	Attack Location ID	A short description of the location under attack, of up to 255 characters.
	Attack Node	A short description of the network node under attack, of up to 255 characters.
	Attack Address	A text field in which you can record the IP address under attack, of up to 255 characters.
Incident Information		
	Incident Source 1	This field is auto-populated.
	Incident Source 2	This field is auto-populated.
	Incident Source Address	A text field in which you can record up to 200 characters.
Vulnerability		
	Vulnerability	This field is auto-populated.
	Vulnerability Type 1	Selections include: Accidental or Intentional.

Field		Description
	Vulnerability Type 2	Selections include: EMI/RFI, Insertion of Data, Theft of Service, Unauthorized, Probes, Root Compromise, DoS Attack, User Account.
	Vulnerability Evidence	This text field can contain up to 4,000 characters.
	Vulnerability Source	This text field can contain up to 4,000 characters.
	Vulnerability Data	This text field can contain up to 4,000 characters.
Other		
	History	Selections include: Known Occurrence and Unknown.
	No. Occurrences	A numeric value; the number of occurrences of the incident.
	Last Occurrence Time	The date and time of the most recent incident.
	Resistance	Selections include: High, Low, and Unknown.
	Consequence Severity	This field is auto-populated.
	Sensitivity	This field is auto-populated.
	Recorded Data	This text field can contain up to 4,000 characters.
	Inspection Results	This text field can contain up to 4,000 characters.
	Conclusions	This text field can contain up to 4,000 characters.

Events Tab

You can add events to a case from the Active Channels page (), as described in Using Active Channel Grids. The system then displays these events on the Cases Events tab.

Field	Description
Description	This field is auto-populated from events included in a case.
Event Info and Payload fields	For selected events, this field displays event values and payload fields, if available.

Events related to a use case are preserved in the case for tracking purposes even after the time period where the events would typically *age out* of the database.

Attachments Tab

The Attachments tab shows files associated with the selected case. Click the **Attach** button to attach another file to the case.

If you do not see files as expected, try clicking the Refresh button () to update the view to show recently added files.

Field		Description
Local file		Select this option to choose a file on your local system. Specify values for the following fields, which are displayed when you choose a local file:
	Name	A descriptive name for the file. This name can differ from the actual file name, and can include spaces. If you do not provide an alternative name here, the original file name is used.
	Description	A text description of the file.
	File	Click Browse and use the file browser to navigate to and select the local file you want to attach to the case. (This field requires user input.)
	Text Encoding	Encoding type. The default is ISO-8859-1.
	Share this file in ArcSight	Click this option if you want to make the file available as a shared resource on the ArcSight Manager.
ArcSight file		Select this option to choose a file on the ArcSight Manager.
	Files to attach	Click the plus button next the drop-down menu to show the file browser on the ArcSight Manager. Navigate to and select a file on the ArcSight Manager. (This field requires user input.)

Click **Attach** to attach the file to the case. (Or click Cancel to abandon attachment edits.)

Click **Submit** to save the case with the new attachment, the same way you save new settings on the other tabs.

Once the file is attached, anyone viewing the case can view details about the file and download it. To do this, navigate to a case, and click the Attachments tab. To view more details about an attachment, click the file name. To download an attachment, click the Download button () for that file.

Notes Tab

Field	Description
Note	Use this field to record notes of up to 4,000 characters.

Chapter 6

Handling Notifications

The Notifications feature displays notifications relevant to you that were triggered by certain event conditions.

The notifications on the display are grouped according to workflow-style stages such as pending, acknowledged, resolved, or informational. The specific groups you see have been tailored to your enterprise.

To see the details of a notification, click its listing in the relevant group.

Notification Categories	Use
Pending	These are notifications that you have not yet handled (reassigned to one of the following categories). Pending notifications older than 24 hours are automatically refiled as Not Acknowledged.
Acknowledged	These are notifications to which you have responded.
Not Acknowledged	Pending notifications that go unacknowledged or unresolved for more than 24 hours are automatically refiled as Not Acknowledged.
Resolved	These are notifications for which you or a colleague have found a resolution and so have marked the notification accordingly.
Informational	These are notifications that are provided for information purposes only and do not require resolution or response.

Chapter 7

Using Reports

The ArcSight Web interface enables you to run reports, and view and save the report results.

The reports available to you are organized in the Cases resource tree on the left. Click the group folders in the tree to open or close them. Click a folder to see a list of its cases in the right-hand pane. Click the arrow icon in the upper-right corner of the resource pane to hide it or show it.

Running and Viewing Reports

To run and view a report

1. Click **Report Definitions** just below the toolbar.
2. Navigate to a report in the resource tree.
3. Click a report definition name to show it in the right pane.
4. Use the values already defined for the report's parameters or change them as necessary. (See "Report Parameters" on page 104.)
5. Click **Run Report** to run the report and display the results.

   If you are running the context report from the event inspector, click **View Report** to run and display the report.

For tips about how to run large reports that make efficient use of system resources, see "Advanced Configuration for Report Performance" on page 106.

Running and Saving Archived Reports

To run and save a report

1. Click **Report Definitions** just below the toolbar.

2 Navigate to a report in the resource tree.

3 Click a report definition name to show it in the right pane.

4 Use the values already defined for the report's parameters or change them as necessary. (See “Report Parameters” on page 104.)

5 Select the **Save Output** checkbox to expose the archive report detail fields.

If you are archiving the context report from the event inspector, click **Archive Report**. The report will generate and be displayed in the viewer panel. You can save the report output using the browser Save As function.

6 Enter the following details for saving the report output as an archived report and click **Run Report**:

Field	Enter this
Archive Report Folder	Browse to an existing folder in the ArcSight file system to save the report results. This makes the report results retrievable from the Archived Reports view later. If you do not select a folder, you can save the report once the results are displayed using the save method that applies to the report format. For example, if you chose PDF, you can use the PDF save to save the results.
Archive Report Name	Accept the default report name or enter a name for the saved report results. Spaces are OK.
Archive Report Expiration Time	Accept the default date (6 months from today), or enter a date when the archived report results are deleted. `$NOW` indicates that the report results will be deleted when you close the report results viewer.

Report Parameters

The following parameters are common to most reports. Depending on the query used as the source for a report, other parameters may be exposed here. For example, a report might prompt for a Start and End Date (timestamps) over which to run the report.

Parameter	Use
Report Format	The format in which to generate the report. Note that RTF appears by default in Word documents, XLS in Excel worksheets, CSV in Excel worksheets, and PDF and HTML in browser windows. The CSV-Plain format intentionally has fewer report header lines.
Page Size	Choose a standard paper size for the printed report (whether you send it directly to print or not).
Run as User	As an option, choose an existing ArcSight user's identity as a report constraint. The user identity can serve as a type of filter on the report's output, or it may be desirable to run a report on behalf of a user, as in a provider/customer (MSSP) circumstance.
E-mail to	Select one or more e-mail addresses to send notifications to when the report runs.
E-mail Format	Choose to send the generated report or a URL to the file.

Parameter	Use
Save Output	Select this option to save the generated report to the ArcSight Manager as an Archived Report. When you select the Save Output option (toggled "on"), provide the name, location, and expiration date of the archived report.
Archive Report Folder	Indicate the name of the folder in which you want to store the report.
Archive Report Name	Enter the name of the report. You can use Velocity Template references here. By default, the report names is set to: `${Today}/${ReportName}_${Now}` **$CurrentDateTime**: Prints the current date and time. (Same as $Now) **$CurrentDate**: Prints the current date. **$CurrentMonth**: Prints the current month. **$CurrentWeek**: Prints the current week. **$Now**: Prints the current date and time. (Same as $CurrentDateTime) **$CurrentDateTime-<Number>**: Prints the current date and time minus the number of days you specify.
Archive Report Expiration Time	Enter an expiration date and time for the archived report. Click the calendar button next to the date field to get a popup calendar in which to designate the date. The ArcSight system automatically removes expired reports.

Viewing Archived Reports

To view an archived report

1. Click **Archived Reports** just below the toolbar.
2. Navigate to a report in the resource tree.
3. Click the name of an archived report to show it in the right pane.

Downloading an Archived Report

To download an archived report

1. Click **Archived Reports** just below the toolbar.
2. In the Download column for the report archive you want, click the **Download** icon.
3. In the File Download dialog box, choose to open the file or save it to a particular location.

Adding New Archived Reports

To add a new archived report to a folder

1. Click **Archived Reports** just below the toolbar.
2. In the resource tree, select the report folder to which you want to add the new archived report.

3 Above the list of available reports, click **New Report**.

4 In the Upload Report screen, enter a report name and specify the path to its file, or click **Browse** to locate it.

5 Click **Upload** to add the archived file to the others available in the folder.

Deleting Archived Reports

To delete archived reports

1 Click **Archived Reports** just below the toolbar.

2 Navigate to a report folder in the resource tree.

3 In the list of archived reports on the right, check those you want to delete.

4 Click **Delete** to remove the checked reports, then click **OK** to confirm.

Advanced Configuration for Report Performance

Reports with large file sizes or large time ranges may require special configurations at the Manager to ensure system performance.

Set these parameters only as needed if you encounter large or complex reports that repeatedly cause performance problems or cause the Manager to restart when you try to run them. Refer to the *ArcSight Administrator's Guide* for more information on setting server properties on the Manager. The properties described here are also documented in the `server.properties` file itself.

Configurations for Large Reports

A very large report (for example, a 500 MB PDF report) might require so much virtual machine (VM) memory that it can cause the ArcSight Manager to crash and re-start.

To prevent that, set up the Manager to expose a special report parameter for generating the report in a separate process. The separate process has its own VM and heap, so the report is more likely to finish. Even if the memory allocated is still not enough, the report failure will not crash the Manager.

This option must be set up on the ArcSight Manager to expose it in the ArcSight Web report parameters list. On the ArcSight Manager in the `server.properties` file, set `report.canarchivereportinseparateprocess=true`. Save the `server.properties` file and restart the Manager.

Once this property is set to "`true`" on the Manager, the Save Output options for a selected report on ArcSight Web include a new parameter called *Generate Report In Separate Process*. Select this option for a report you want to archive as a separate process, and run the report.

If a report is saved with the parameter set to "`true`", the report is archived as a separate process even if the property `report.canarchivereportinseparateprocess` in `server.properties` is set back to "`false`" later on.

Configurations for Reports with Large Time Ranges

Reports that query over a large time range with complex joins run much faster if the query contains a full scan database hint. This option must be set up on the Manager to expose it in the ArcSight Web report parameters list.

On the ArcSight Manager in the `server.properties` file, set `report.canquerywithfullscanhint=`**`true`**. Save the `server.properties` file and restart the Manager.

Once this property is set to "`true`" on the Manager, the Save Output options for a selected report on ArcSight Web include a new parameter called *Query with Full Scan Hint*. Select this option for a report you want to run with the full scan hint, and run the report.

If a report is saved with the parameter set to "`true`", the report is archived as a separate process even if the property `report.canquerywithfullscanhint` in `server.properties` is set back to "`false`" later on.

Chapter 8

Monitoring Dashboards

The ArcSight Web interface enables you to view dashboards made available from the ESM Console.

When you click **Dashboards** in the toolbar, you see the Dashboards display, usually with the Dashboards tree open in the resource pane and the dashboards of the current branch listed in the content pane.

"Viewing and Managing Dashboards" on page 109

"Changing Dashboard Layouts" on page 109

Viewing and Managing Dashboards

The dashboards are organized in the resource tree on the left. Click the group folders in the tree to open or close them. Click a folder to see a list of its dashboards in the pane to the right. Click the arrow icon in the upper-right corner of the resource pane to hide or show it.

Click a dashboard's name to open it and its collection of data monitors in the right pane.

By default, the information on a dashboard refreshes automatically every 60 seconds. Click the "Pause" button (**| |**) to stop refreshing, or click the circular arrow to refresh immediately. Click the arrow head to resume auto-refreshing.

Run the mouse pointer over elements in graphic data monitors to see their details in tooltips.

Three types of data monitors are available through ArcSight Web: Event Graph, Geographic Event Graph, and Hierarchy Map.

Changing Dashboard Layouts

You can change the way data monitors are laid out on dashboard displays. When you click **Dashboards** and choose one to show from the resource tree, the layout of data monitors in the right panel is a default pattern.

In a dashboard display, click **Edit Layout** to open the Dashboard Layout editor.

To rearrange data monitors, click and drag them from one of the display areas to another. The upper and lower "wide" areas are intended to better accommodate tables, which most often run wide and cannot be resized. The left and right "narrow" areas are intended to accommodate charts, which are more likely to resize successfully.

To see a rearrangement, click **Save**.

Chapter 9

Using the Knowledge Base

ArcSight Web provides access to viewing knowledge base articles. The articles available to you are organized in the resource tree on the left. Click the folders in the tree to open or close them. Click the arrow icon in the upper-right corner of the resource tree panel to hide it or show it.

ArcSight offers the Knowledge Base as a convenience for storing user-generated pointers or articles of interest. It is not pre-populated.

Chapter 10

Using Reference Pages

An event viewed from the Event Inspector may have a reference page associated with it. The contents of a reference page is set through the ArcSght Console.

- If present in an event, click **View references** to show the reference page content in a separate browser window.
- Use the drop-down menu to navigate or other pages of this reference if more pages are available.
- Use the browser's **Back** button to return.

Chapter 11

Setting Preferences

In any display, click **Options** in the toolbar to set or change your preferences for date formatting, locale, active channel startup, and password.

Click the **Formats** tab to choose the style and punctuation to use for date and time values. Click Update to apply your changes before moving to another tab.

Click the **Locale** tab to choose the time zone you work in. Click **Update** to apply your changes before moving to another tab.

Click the **Channels** tab to set, or bypass setting, the parameters for active channels, each time you open one. The check box is clear by default, which means that you will see the channel setup options. Select the check box to avoid setup and to go directly to the channel display. There is also an option to hide (collapse) the channel tree on the left panel when a channel is already running. By default, this tree remains in view. Click **Update** to apply your changes before moving to another tab.

Click the **Password** tab to change your current password. Enter your old password first. Then enter your new password and repeat it to confirm. Click **Update** to put your change into effect.

Chapter 12

Custom Branding and Styling

You can change logo images, colors, and styles for ArcSight Web by creating and editing the file `<ArcSightWeb_HOME>/config/web/styles.properties`.

This file doesn't exist by default, but you can create it by copying either `example.styles.properties` or `full.styles.properties` and renaming it to **styles.properties**.

Please do not modify the file `<ArcSightWeb_HOME>/config/web/styles.defaults.properties`. This file contains the default settings. It will be overriden by your custom `styles.properties` file.

The properties file provides information about those properties that can be changed, along with example values.

To add custom branding or styles:

1. Modify the properties in `styles.properties` as needed to fit your custom branding and style requirements, and remove the comment tags from the lines that contain property settings you want to apply.
2. If you want to add one or more custom logo images as part or your re-branding effort, you will need to both both modify the relevant property settings and add the image(s) to the `webapp/images` directory:
   - Modify the properties file to call your custom image file(s) and un-comment the relevant lines (e.g., `navbarLogoImg=MyCustomLogo.gif` and `loginLogoImg=logo-login-MyCustomLogo.gif`). You might also want to modify and un-comment the logo image size property and navigation bar text colors to make the proper customizations.
   - Add the image file to the directory `<ArcSightWeb_HOME>/webapp/images`.
3. Restart ArcSight Web to see the effects of your custom changes.

Remember that branding changes are visible to anyone using that instance of ArcSight Web. You can, however, run multiple instances of ArcSight Web against the same ArcSight Manager.

Index