

HP ArcSight Logger in 2 Hours

An introduction to conducting forensic investigations
Using ArcSight Logger 6

Failed Logons Use Case



Reducing complexity, cost and risk in your security infrastructure

By: Brian Wolff
CISSP, MBA
HP ArcSight
ArcSight Architect, Americas

December 16, 2014

Table of Contents

- 1. Summary.....3
- 1.1. Document History3
- 1.2. Current models of Logger4
- 2. ArcSight Logger Trial, Downloads and Demos5
- 3. Deployment Scenarios7
- 4. Logger Appliance Configuration8
- 5. Introduction to Logger13
- 5.1. Introduction to the interface15
- 6. Connecting to the Logger User Interface16
- 7. Prepare System for Use Case Below23
- 7.1. Configuring Logger to accept the Windows Unified Connector Events.....23
- 7.2. Configuring the Windows Unified Connector to collect and send events to a Logger appliance.....25
- 7.3. Installing the Windows Unified Connector to collect and send events to a Software Logger.....28
- 8. USE CASE Step by Step.....33
- 8.1. Search / Analyze33
- 8.2. Categorization35
- 8.3. Viewing a Live Feed42
- 8.4. Dashboards43
- 8.5. Reporting.....48
- 8.6. Running a default report49
- 8.7. Creating a report, by customizing default report.....51
- 9. Pipeline Operators:60
- 10. Selected Examples:.....61
- 11. Reporting Example.....68



1. Summary

Secure Your Data, Enforce Compliance, and Defeat Cybercrime

Get Started in Minutes!

ArcSight Logger is available as free downloadable software that brings true enterprise-class log management functionality to everyone. Users can download, install and start getting instant value out of their logs within minutes. Using this version, you can collect up to 750 MB of log data per day and store up to 500 GB of uncompressed logs (assuming average compression 10:1). It also comes with 90 days of phone and email support followed by access to the ArcSight Logger user community. As shown below, the downloadable version of ArcSight Logger provides access to all enterprise features for a full 12 months. Anytime during that period, you can upgrade to an enterprise version.

What It Does

ArcSight Logger collects information from any system that generates log data. It can process that information as much or as little as desired, and can produce ultra-fast searching across the data. As a result, organizations of any size can use this high performance log data repository to aid in faster forensic analysis of IT operations, application development, and cyber security issues, and to simultaneously address multiple regulations.

How It's Different

Until now, log analysis was asset-centric and organizations purchased one product for security and compliance reporting, a different product for IT operations search and yet another one for application development. Today, the questions that need to be answered through log analysis are increasingly user-centric and can span any and all infrastructure. Traditional log management tools cannot be expanded to analyze logs across the enterprise because they are limited by the type of sources; have restricted search/reporting capabilities and are not scalable.

ArcSight Logger is a universal log management solution that can capture and analyze ALL enterprise log data to answer questions of individual teams and can easily be expanded into an enterprise-wide log management solution when needed.

1.1. Document History

Initial Release Based on ArcSight Logger 5.2

Update: 2012/11/08 Modified for Windows 2008 logs

Please refer any documentation changes or suggestions to brian.wolff@hp.com

Update: 2014/04/10 for Logger 5.5

Update: 2015/12/17 for Logger 6



1.2. Current models of Logger

ArcSight Logger is available as Software or as an Appliance.

<http://www8.hp.com/us/en/software-solutions/arc-sight-logger-log-management/tech-specs.html>

The current models of the Logger Software available are:

ArcSight Logger Software Specifications

Model (E-LTU)	Max log volume	Max Online Storage	Max data volume/instance	Max instances in peering	Max data volume
HP ARST Logger 5GB/d SW (Base + Add-on)	5 GB/ day each	8 TB	250 GB/ day	20	5 TB/ day

Software Generic Specs

Supported OS	Red Hat Enterprise Linux v6.5, 64-bit CentOS v 6.5 64-bit
Recommended Hardware	CPU: 2 x Intel Xeon Quad Core or equivalent Memory: 12 - 24 GB (24 GB recommended) Disk Space: 65 GB (minimum) in the software Logger installation directory. If you allocate more space, you can store more data. Root partition: 400 GB Temp directory: 1 GB
Storage	Average compression of 10:1 (depending on the data type and source)

The current models of the Logger Appliance available are:

ArcSight Logger Appliance Specifications

Model	L3505	L7505-SAN	L7505s	L7505x
Daily Data Limits (not expandable)	30 GB/day	160 GB/day	80 GB/day	160 GB/day
Capacity (Compressed Data)	800 GB	8TB	8TB	8TB
Hardware Spec	1x Intel Xeon, E5-2620 2.0GHz, 6-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor
Memory	32 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM
Storage	4 x 500 GB (1.5 TB RAID-5)	External - SAN	4 x 3 TB (9 TB - RAID 5)	4 x 3 TB (9 TB - RAID 5)
Host Bus Adapter	N/A	2 x 2-port 16 GB Emulex HBA	N/A	N/A
Dimensions (DxWxH)	27.5" x 17.1" x 1.7"	27.5" x 17.1" x 1.7"	29.5" x 17.1" x 1.7"	29.5" x 17.1" x 1.7"
Connector Management	Yes	N/A	N/A	N/A

Generic Specs

Management	Web browser, CLI, Web Services API
Operating System	Red Hat Enterprise Linux v6.5, 64-bit
Supported Sources	Raw Syslog (TCP/UDP), Raw File based logs (FTR, SCP, SFTP) Analysis optimized collection using HP ArcSight SmartConnectors FlexConnector framework for legacy event sources HP ArcSight CEF (Common Event Format), HP ArcSight ESM
Storage	Average compression of 10:1 (dependent on data type and data source)
Power	2 x 460W CS Platinum Power Supply
Ethernet Interfaces	4 x 10/100/1000
Chassis	1U



2. ArcSight Logger Trial, Downloads and Demos

Logger is delivered in several formats

1. Appliance Logger
2. Software Logger
3. Trial Logger 6.0 for Linux
4. Trial Logger 6.0 on VMware VM

Below is the link for the free trial license of (2) Software Logger.

ArcSight Logger is now available as a Limited Period, no cost demo. You can locate it at the following link, which is also seen in the screen-shot that follows:

<http://www8.hp.com/us/en/software-solutions/arcsight-logger-log-management/try-now.html>

The screenshot shows the HP ArcSight Logger 6.0 English SW E-Media trial page. The page is divided into several sections. At the top, there is a blue header with the HP logo and navigation links for 'For Home', 'For Work', and 'Support'. Below the header is a navigation bar with icons for 'Software Home', 'Security', 'Service & Portals', 'Big Data Analytics', 'Automation & Cloud', 'Business Service Management', 'Mobile', and 'App Lifecycle'. The main content area is titled 'ARCSIGHT LOGGER TRIAL, DOWNLOADS AND DEMOS' and includes a 'Download Now' button. A 'Tell us about yourself' form is visible on the right side of the page. A red arrow points to the 'Download Now' button, and another red arrow points to the 'Click to enlarge' link below a screenshot of the software interface.



hp For Home For Work Support Search HP.com

Software / Log Management Tools, ArcSight Logger

1 Overview > 2 Terms of service > 3 Download

HP ArcSight Logger 6.0 English SW E-Media

Software Download Terms of Use

READ CAREFULLY BEFORE DOWNLOADING THE SOFTWARE.

1. This license agreement (the "Agreement") states the terms between you ("You" or "Your") and Hewlett-Packard Company and its Subsidiaries ("HP") for the software that You download from HP's website (the "Software"). By downloading, copying, or using the Software You agree to this Agreement. If You do not agree to be bound by the terms of this Agreement, do not click on "I Agree" below and do not download, install, copy, or use the Software.
2. Terms. This Agreement includes supporting terms and information referenced by HP, which may be software license information, additional license authorizations, software specifications, published warranties, supplier terms, open source software licenses and similar content ("Supporting Materials"). Additional license authorizations are available at: www.hp.com/go/SWLicense.
3. Authorization. If you agree to this Agreement on behalf of another person or entity, you warrant you have authority to do so. This Agreement will be enforceable against You and any entity for which you download, install or use the Product.
4. Consumer Rights. If you obtained the Software as a consumer, nothing in this Agreement affects your statutory rights.
5. License Grant. As long as you comply with this Agreement, HP grants you a non-exclusive non-transferable license to use one copy of the version or HP LICENSE, AVAILABLE AND SUBJECT TO YOUR ACCEPTANCE OF THE HP SOFTWARE DOWNLOAD AGREEMENT, IF YOU CLICK "DISAGREE" AND DO NOT ACCEPT THE HP SOFTWARE DOWNLOAD AGREEMENT, THEN YOU ARE NOT GRANTED ACCESS TO THE SOFTWARE, YOU ARE NOT AUTHORIZED TO USE THE SOFTWARE, AND YOU MAY NOT DOWNLOAD THE SOFTWARE.

I DISAGREE I AGREE

hp For Home For Work Support Search HP.com

Software / Log Management Tools, ArcSight Logger

1 Overview > 2 Terms of service > 3 Download

HP ArcSight Logger 6.0 English SW E-Media

You may now download your software and supporting materials.

For License keys or to download content again, please refer to our download confirmation email sent to bfles.wolf@hp.com. Review our [FAQ](#) for more helpful information.

Name	File Size	Using HP Download Manager
HP ArcSight Trial Logger 6.00 for Linux	286 MB	Download
HP ArcSight Trial Logger 6.00 on VMware VM	702 MB	Download
HP ArcSight SmartConnectors for Logger Trial	340 MB	Download

You might also like the following:

Get community support for ArcSight Logger
Get Started with ArcSight Logger
Watch ArcSight Logger in action. (6:48 minutes)

United States

United States

h20392.www2.hp.com/eCommerce/akam/tableviewpopup.html?language=en&r=0.5769607165002217&urls=http%3A%2F%2Fh30537.www3.hp.com%2Fdownloads%2FHFP_ArcSight_Sm

Progress	Size	Status	Filename
52.3%	348.12 MB	DOWNLOADING	HP_ArcSight_SmartConnectors_for_Logger_Trial_HP-ArcSight-SmartConnectors-for-Logger-Trial.zip

h20392.www2.hp.com/eCommerce/akam/tableviewpopup.html?language=en&r=0.0249316006048941&urls=http%3A%2F%2Fh30537.www3.hp.com%2Fdownloads%2FHFP_ArcSig

Progress	Size	Status	Filename
13.7%	702.96 MB	DOWNLOADING	HP_ArcSight_Trial_Logger_6.00_on_VMware_VM_HP-ArcSight-Trial-Logger-600-on-VMware-VM.zip

h20392.www2.hp.com/eCommerce/akam/tableviewpopup.html?language=en&r=0.783458062630865&urls=http%3A%2F%2Fh30537.www3.hp.com%2Fdownloads%

Progress	Size	Status	Filename
34%	286.03 MB	DOWNLOADING	HP_ArcSight_Trial_Logger_6.00_for_Linux_HP-ArcSight-Trial-Logger-600-for-Linux.zip

WinZip [HP_ArcSight_Trial_Logger_6.00_for_Linux_HP-ArcSight-Trial-Logger-600-for-Linux.zip]

- ArcSight-logger-6.0.0.7285.0.trial.bin
- ArcSight-logger-6.0.0.7285.0.trial.bin.sig
- ArcSight-logger-6.0.0.7285.0-opensource.tgz
- Logger_AdminGuide_6.0.pdf
- Logger_QuickStart_Trial_6.0.pdf
- Logger_RelNotes_6.0.pdf
- Logger_WebServicesAPI_6.0.pdf

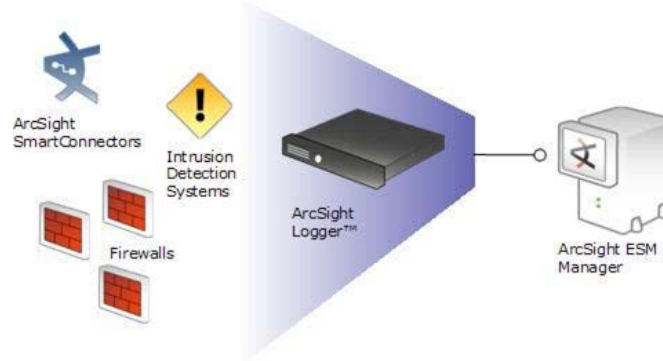


3. Deployment Scenarios

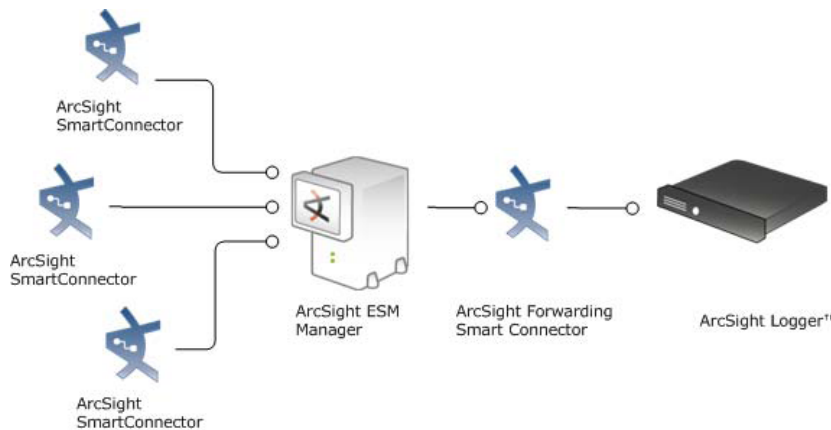
Typically, Logger is deployed inside the perimeter firewall with a high degree of physical security to prevent tampering with the collected event information. Logger does not require other ArcSight products. It receives and forwards syslog and log file events created by a wide variety of hardware and software network products. Logger also interoperates with ArcSight ArcSight's Enterprise Security Manager (ESM) correlation product as shown in the following figures. A typical use of Logger is to collect firewall or other data and forward a subset of the data to ArcSight ESM for real-time monitoring and correlation, as shown below. Logger can store the raw firewall data for compliance or service level agreement purposes.



In the following illustrations ArcSight Logger can be the Logger appliance or the software version of Logger that is installed on a supported platform of your choice.



Logger can act as a funnel, forwarding selected events to ArcSight ESM.



Logger can store events sent by ArcSight ESM.



4. Logger Appliance Configuration

These are some common configuration tasks that should be understood when setting up a Logger Appliance.

4.1.1. Configure Network Settings on a Logger

Below are instructions on how to set an IP address and a default gateway on a Logger Appliance.

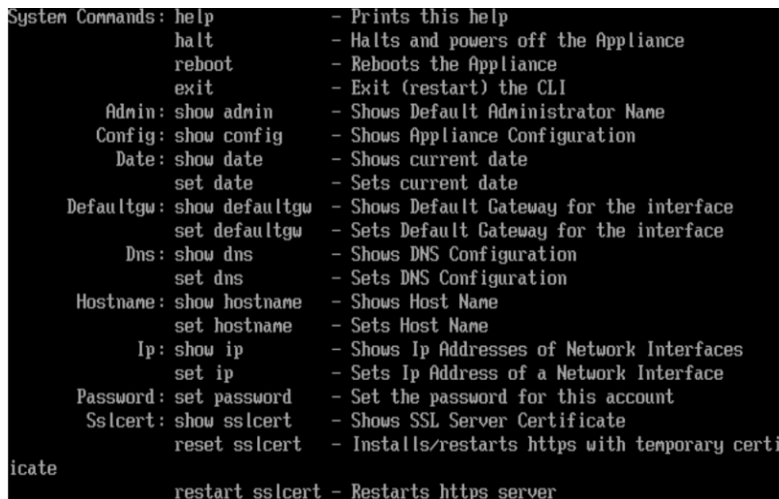
- 1) Attach a KVM or Keyboard, Monitor and Mouse to the appliance after it is fully booted and login as the default user interface credentials:

Username: *admin*

Password: *password*



- 2) Type “help” if you want to display a help screen with a list of commands and descriptions.



```
System Commands: help - Prints this help
                  halt - Halts and powers off the Appliance
                  reboot - Reboots the Appliance
                  exit - Exit (restart) the CLI
Admin: show admin - Shows Default Administrator Name
Config: show config - Shows Appliance Configuration
Date: show date - Shows current date
      set date - Sets current date
Defaultgw: show defaultgw - Shows Default Gateway for the interface
           set defaultgw - Sets Default Gateway for the interface
Dns: show dns - Shows DNS Configuration
     set dns - Sets DNS Configuration
Hostname: show hostname - Shows Host Name
         set hostname - Sets Host Name
Ip: show ip - Shows Ip Addresses of Network Interfaces
   set ip - Sets Ip Address of a Network Interface
Password: set password - Set the password for this account
Sslcert: show sslcert - Shows SSL Server Certificate
         reset sslcert - Installs/restarts https with temporary certificate
         restart sslcert - Restarts https server
```

- 3) **Set the IP address:** You can show the usage of how to set the IP by simply typing “set IP”.



```
logger> set ip
Usage: set ip <interface> <ip address>[/prefix] [netmask]
```



- 4) Set the IP address based on the usage output. This example below sets the IP of the eth0 interface to 10.0.187.38 with a netmask of 255.255.255.0.

```
logger> set ip eth0 10.0.187.38 255.255.255.0
```

- 5) Type “show ip” to verify the IP is set properly for eth0.

```
logger> show ip eth0
eth0      Link encap:Ethernet  HWaddr 98:4B:E1:74:A9:30
          inet addr:10.0.187.38  Bcast:10.0.187.255  Mask:255.255.255.0
          inet6 addr: fe80::9a4b:e1ff:fe74:a930/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38  errors:0  dropped:0  overruns:0  frame:0
          TX packets:42  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:3472 (3.3 KiB)  TX bytes:3132 (3.0 KiB)
          Interrupt:162  Memory:f4000000-f4012800
```

- 6) **Set the default gateway:** You can type “set defaultgw” to show usage on how to set the default gateway.

```
logger> set defaultgw
Usage: set defaultgw <gateway ip> [interface]
```

- 7) Based on the usage info, set the default gateway. This example sets the default gateway to 10.0.187.1 for interface eth0.

```
logger> set defaultgw 10.0.187.1 eth0
```

- 8) Verify the default gateway by typing “show defaultgw”.

```
logger> show defaultgw
Destination      Gateway          Genmask          Flags Metric Ref      Use Iface
default          10.0.187.1      0.0.0.0          UC      0      0        0 eth0
```

- 9) Connect to the Logger from a workstation to confirm the configuration.

<https://10.0.187.38> (in this example only)



4.1.2. Installing a license on Logger Appliance

*Note the Limited Use Free License is automatically deployed, you do not need to do this step

1 Connect to the appliance's user interface.

<https://10.0.187.38> (in this example)

Default ID and Password: admin/password

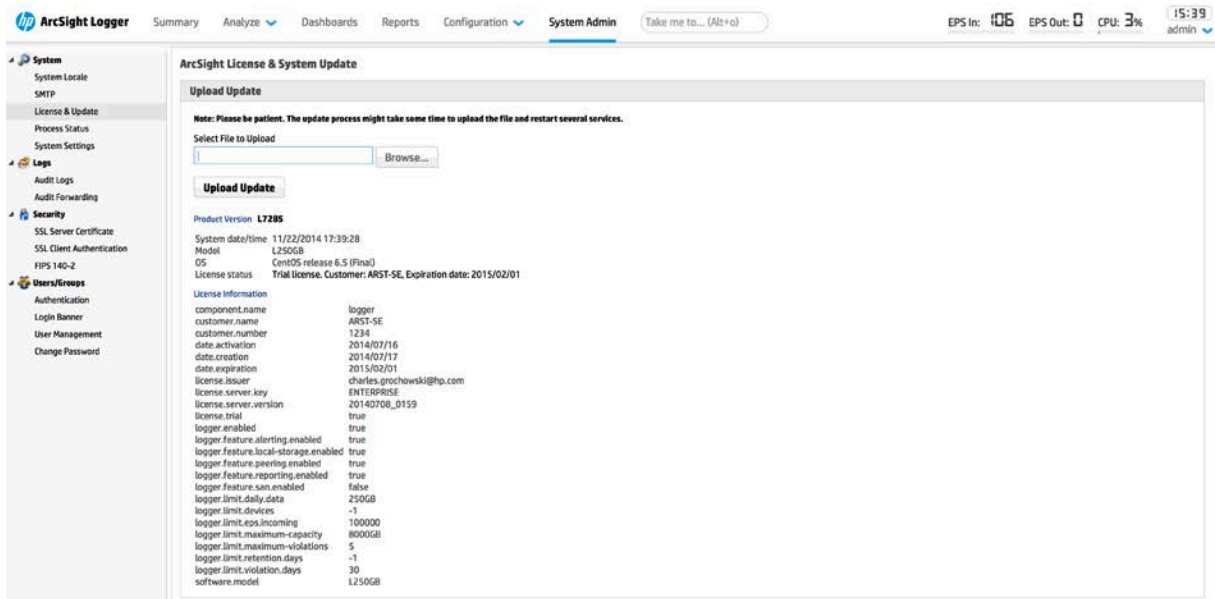
You will need to read through the user agreement before checking the “Accept” box.

2 Click **System Admin** from the top-level menu bar.

3 Click **License & Update** from the System section.

4 Click **Browse** to locate the file.

5 Click **Upload Update**.



The screenshot shows the HP ArcSight Logger web interface. The top navigation bar includes 'System Admin' and a search box. The left sidebar shows a tree view with 'System Admin' expanded to 'License & Update'. The main content area is titled 'ArcSight License & System Update' and contains an 'Upload Update' section with a 'Select File to Upload' field and a 'Browse...' button. Below this is a 'License Information' table with the following data:

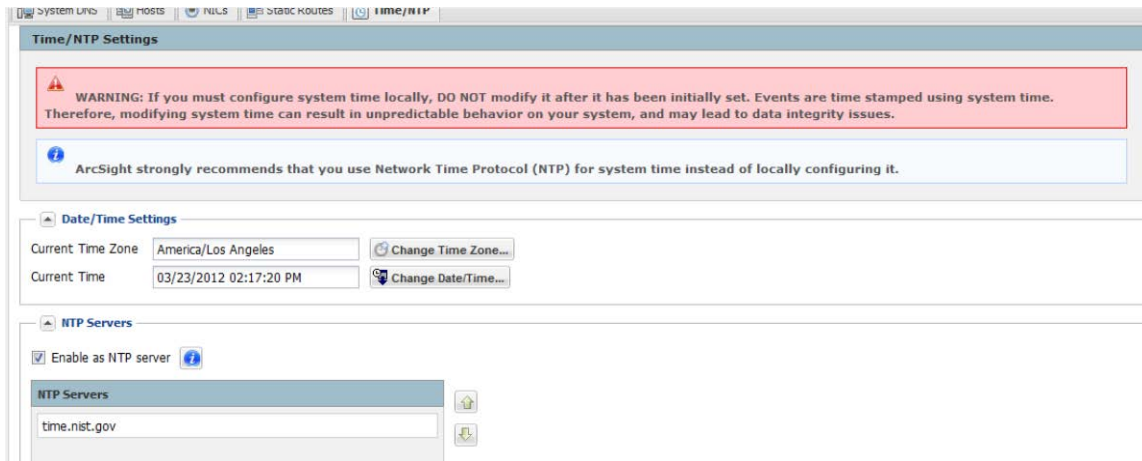
License Information	
component.name	logger
customer.name	ARST-SE
customer.number	1234
date.activation	2014/07/16
date.creation	2014/07/17
date.expiration	2015/02/01
license.issuer	charles.grochowski@hp.com
license.server.key	ENTERPRISE
license.server.version	20140708_0159
license.trial	true
logger.enabled	true
logger.feature.alerting.enabled	true
logger.feature.local-storage.enabled	true
logger.feature.peering.enabled	true
logger.feature.reporting.enabled	true
logger.feature.san.enabled	false
logger.limit.daily.data	250GB
logger.limit.devices	-1
logger.limit.eps.incoming	100000
logger.limit.maximum.capacity	8000GB
logger.limit.maximum-violations	5
logger.limit.restriction.days	-1
logger.limit.violation.days	30
software.model	L250GB

4.1.3. Configuring Date & Time zone

Configuring the date and time zone properly is important so that timestamps on events will come in properly. You can setup the date using an NTP server or set the date & time zone manually here in the user interface:

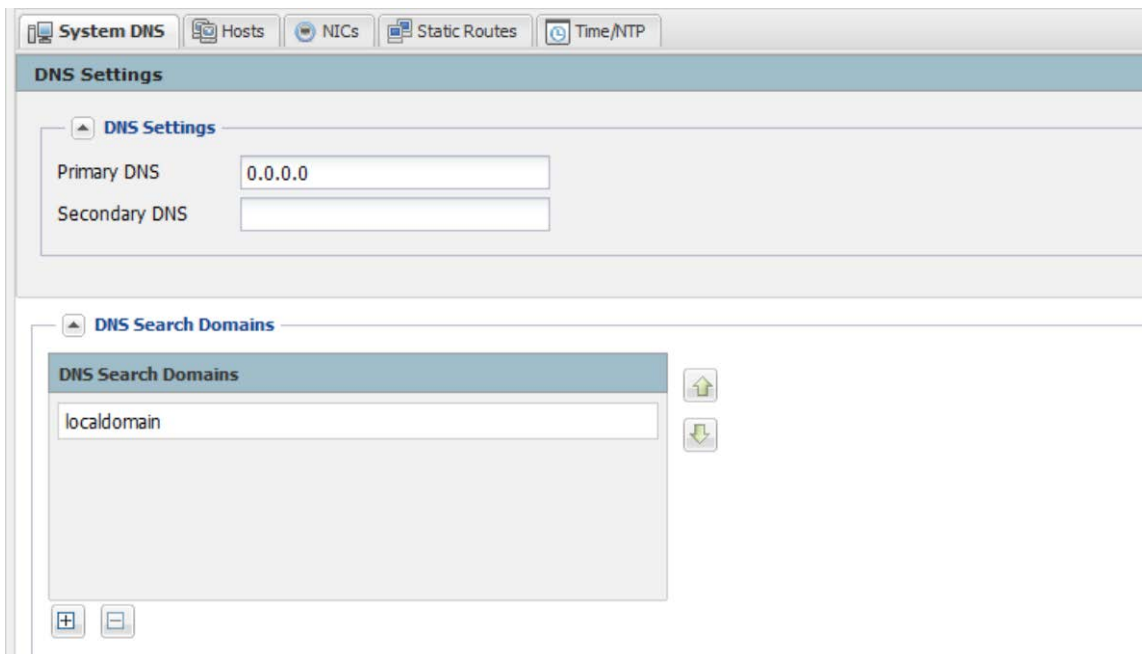
1. Click **System Admin** from the top-level menu bar.
2. Click **Network** from the System section.
3. May need to change the Time Zone by clicking the “Change Time Zone” button and supplying the correct time zone. This will require a reboot.
4. Click the **Time/NTP** tab and enter in your settings. If you use an NTP server it will automatically update the date/time.
5. Click “save” to save your entries.





4.1.4. Configure DNS Settings

1. Click **System Admin** from the top-level menu bar.
2. Click **Network** from the System section.
3. In the **System DNS** tab, enter new values for the IP address of the primary and secondary DNS servers and edit the list of search domains (6 search domains entries is a limit imposed by the OS).
4. Click “Save” to save your entries.



4.1.5. Setup Hosts file entries

Setting up hosts file entries is especially important when configuring Connectors on Connector Appliance with an ESM or Express destination. This is because those destinations usually have certs configured that use a hostname. To configure the hosts file entries, follow these steps:

- 1 Click **System Admin** from the top-level menu bar.
- 2 Click **Network** from the System section.
- 3 In the **Hosts** tab, enter in your hosts entries with the following format:
<ip-address> <hostname>

Example below shows an entry for “esm” host



5. Introduction to Logger

ArcSight Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events.

Logger is available in two form factors: an appliance and software. The appliance-based solution is a hardened, dedicated, enterprise-class system that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis.

Supported Platforms

You can install software Loggers on platforms with the hardware specifications and supported operating systems outlined below, according to the indicated deployment scenarios. This information applies to both physical and virtual machines.

VM installation on the operating systems listed in the table below is supported. Additional information about installing Logger on VMware is available in the Logger for VMware VM Quick Start Guide.



- HP strongly recommends allocating 4 GB RAM per VM instance.
- The sum of memory configurations of the active VMs on a VM server must not exceed the total physical memory on the server.

Specification	Details
Supported Operating Systems	<ul style="list-style-type: none"> • Red Hat Enterprise Linux (RHEL) versions 6.2 and 6.5 (64-bit) • CentOS versions 5.5 and 6.5 (64-bit) <p>Notes:</p> <ul style="list-style-type: none"> • HP ArcSight recommends RHEL 6.5 for fresh installs. • If you are planning to upgrade your current OS and the Logger at the same time, HP ArcSight recommends upgrading the Logger application first followed by the OS. For example, upgrade from Logger 5.3 SP1 to Logger 5.5 followed by an upgrade from RHEL 6.2 to 6.5.
CPU, Memory, and Disk Space	<p>For the Trial Version and VM Instances</p> <ul style="list-style-type: none"> • CPU: 1 or 2 x Intel Xeon Quad Core or equivalent • Memory: 4 - 12 GB (12 GB recommended) • Disk Space: 10 GB (minimum) • Temp directory: 1 GB <p>For the Enterprise Version</p> <ul style="list-style-type: none"> • CPU: 2 x Intel Xeon Quad Core or equivalent • Memory: 12 - 24 GB (24 GB recommended) • Disk Space: 65 GB (minimum) in the software Logger installation directory. If you allocate more space, you can store more data. • Root partition: 400 GB • Temp directory: 1 GB <p>Note: Using NFS as primary event storage on software Logger is not recommended.</p>
Other Applications	For optimal performance, make sure no other applications are running on the system on which you install Logger.

For a detailed capacity planning guide, see the Capacity Planning for Software Version of Logger document that is available for download from the Protect 724 Community at <https://protect724.arcsight.com>.



Connecting to Logger

The Logger user interface (UI) is a web browser application using Secure Sockets Layer (SSL) encryption. Users must log in and be authenticated before they can access the Logger UI.

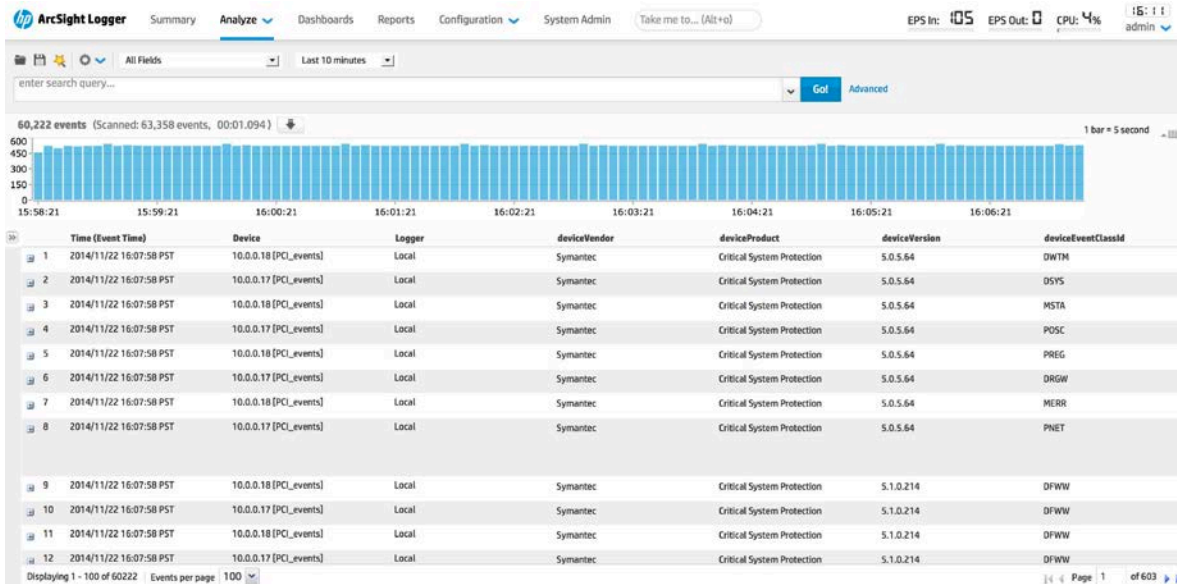
Logger 6.0 supports access through the following browsers:

- **Firefox:** Version ESR 31
- **Internet Explorer:** Versions 10 and 11
- **Chrome:** Latest version
- **Safari:** version 7.0 (on OSX 10.9)

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome includes a Flash player, and so does not need an additional one.) Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is available for free at <http://www.adobe.com/products/flashplayer.html>

JavaScript and cookies must be enabled.

Logger stores time-stamped text messages, called events, at high and sustained input rates. Logger compresses raw data, but can always retrieve unmodified data on demand, for forensics-quality litigation data.



Logger can receive structured events that are parsed and unstructured RAW events, for which no parser is involved. Both types of events are searched for from a common interface.

Logger leverages the ArcSight SmartConnector framework to collect events. Logger can receive normalized CEF events from the SmartConnectors.

Multiple Loggers can work together for scalability purposes, supporting extremely high event volumes. Loggers can be configured as a peer network, with search queries distributed across all loggers.



Syslog is a loose standard (characterized, not defined, in RFC 3164) for event messages.

Although Logger is message-agnostic, it can do more with messages that adhere to the Common Event Format (CEF), an industry standard for the interoperability of event- or log-generating devices currently supported by many technology providers.

Raw Events consist of a receipt time, event time, a source (host name or IP address), and an un-parsed message portion. Logger displays events in a tabular form, as shown above.

Analyzing Events

Events can be searched, yielding a table of events that match a particular query. Queries can be executed manually or automatically, entered into the search field by clicking on terms in the event table. Queries can be based on plain English keywords (full-text search), predefined fields, or specified as regular expressions. Logger supports a flow-based search language that allows you to specify multiple search commands in a pipeline format.

By default, Logger queries only its primary data store even if peer Loggers are configured. However, you can configure Logger to distribute a query across peer Loggers of your choice.

Queries can be saved as a Filter or as a Saved Search. Saved filters can be used to select events for forwarding or to query events again later. For ease of use, Saved Filters and Saved Searches can be quickly called upon by typing "\$" into a search box at any time. This is an enhancement in Logger 6.0 which can collectively save a great amount of time when running multiple queries. A Saved Search is used to export selected events or save results to a file, typically as a scheduled task.

These saved searches are also leveraged to provide dashboards that can be customized to each individual user.

5.1. Introduction to the interface



Browser Requirements

Logger works with most modern browsers, including Internet Explorer (versions 10 and 11), Mozilla Firefox (version ESR 31), and Safari (version 7.0 - on OSX 10.9). Javascript and cookies must be enabled. An Adobe Flash Player plug-in is required for Internet Explorer browsers that access the Logger user interface. Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is

available for free at <http://www.adobe.com/products/flashplayer/>. Please look to the most current Release Notes to find the browser versions supported for your particular release.

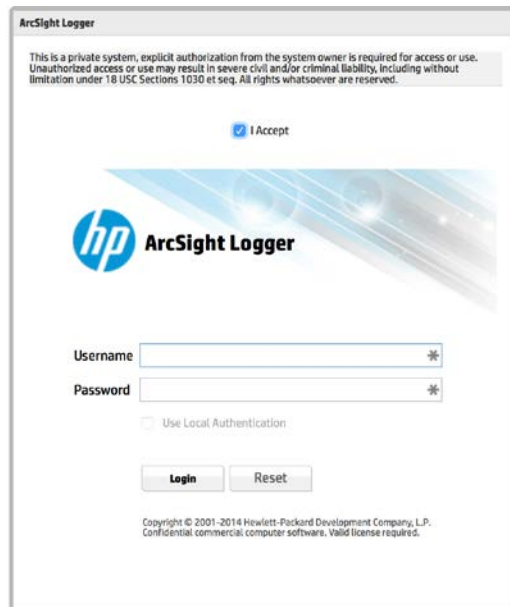
6. Connecting to the Logger User Interface

Because the user interface of the software Logger uses SSL, make sure you connect using https, as seen in the following URL:

https://<hostname or IP address>:<configured_port>

Where hostname or IP address is of the system on which you installed Logger software.

Once you use the URL specified above, the following Login screen is displayed.



Note that your system may have the disclosure enabled, which must be accepted before the login fields are available. This is a configurable option.

For the Logger Limited Use Free Version, use the following information:

Username: admin

Password: password

(Please change after first use)

Navigating the User Interface

As shown below, a consistent navigation and information band runs across the top of every page in the user interface.



Real-time counters, located at the top of the screen, provide an indication of the throughput and CPU usage information, as well as the current time, which are available in more detail on the Monitor Dashboard (“Dashboards” on page 22). The current user-name is also displayed immediately below the time in the top-right corner of the screen.



Help

A help link is found under the admin drop-down, which provides context-sensitive online help related to the currently displayed window-pane.

In addition, Search Helper, a search-specific utility is available that provides search history, search operator history, examples, suggested next operators, and list of fields and operators. Search Helper is available and enabled by default. This helper automatically displays relevant information based on the query currently entered in the Search text box.

Options

The **Options** page enables you to set the default start page (home page) for all users and specific start pages for individual users.

Options

System

EPS input rate gauge max 100K

EPS output rate gauge max 100K

Default start page for all users Summary

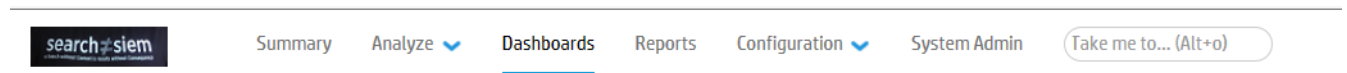
Upload a logo (PNG file) No file selected.

Show default logo

Personal

Default start page for admin Use default for all users

Logger 6 also added the option to add your own logo. I added this as my logo. Feel free to use this or your own company logo.



Logout

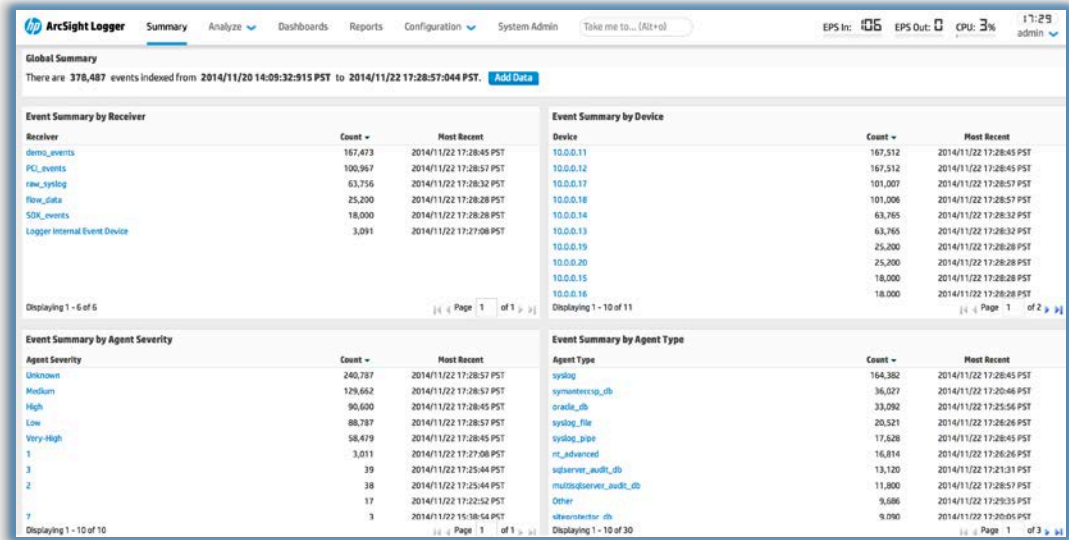
Click the Logout link on any page to return to the Login screen. Logging out is good security practice, to eliminate the chance of unauthorized use of an unattended Logger session.

Logger automatically logs you out after a user-configurable length of time (15 minutes by default). To change this length of time, see the Logger Administrator's Guide.

Summary

The Summary page is a global dashboard that provides summarized event information about your Logger in one screen. It enables you to gauge incoming events activity and the status of indexing.





Dashboards

Dashboards are an all-in-one view of the Logger information of interest to you. You can assemble various search queries that match events of interest to you, status of Logger components such as receivers, forwarders, storage, CPU, and disk, or a combination of both on a single dashboard for status at-a-glance.

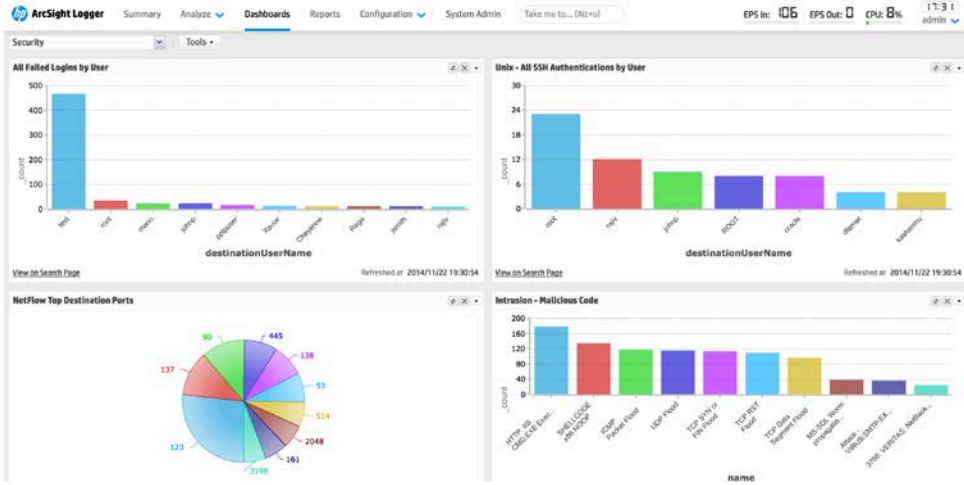
Each Dashboard contains one or more panels of these types: Search Results and Monitor.

The Search Results panel displays events that match the query associated with the panel.

The Monitor panel displays the real-time and historical status of various Logger components such as receivers, forwarders, storage, CPU, and disk.

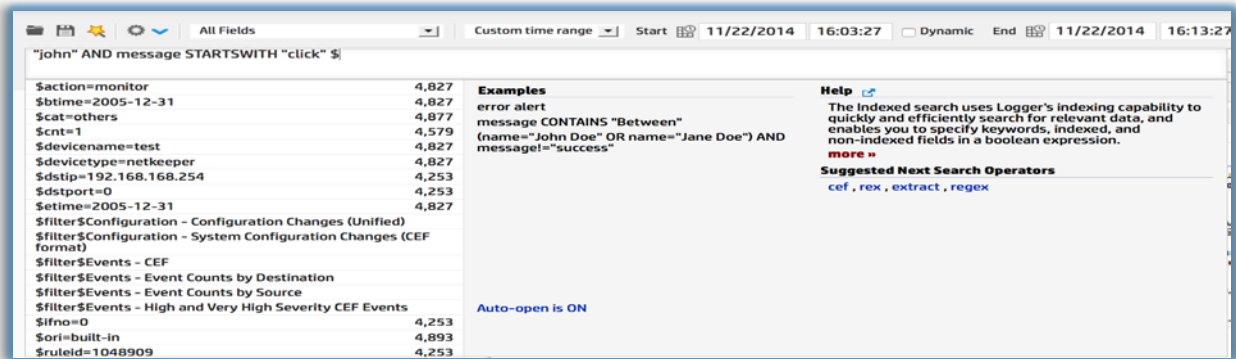
For more details about Dashboards, see the Logger Administrator’s Guide.

Example:



Searching and Analyzing Events

The Process of Searching Events through stored events is very simple and intuitive on Logger. It uses a flow-based search language that allows you to specify multiple search commands in a pipeline format. In addition, you can customize the display of search results, view search results as charts, and, as always, access saved searches and filters with “\$”.



Next, enter the keywords or information you are searching for (referred to as queries) in the Search text box, select the time range, and click Go, as shown in the previous figure. Logger searches for the data that matches the criteria you specified and will display the results on the same user interface page where you entered your query.

A query can be as simple as a keyword; for example, `hostA.companyxyz.com`. Or a complex query that includes Boolean expressions of keywords and indexed fields, and regular expressions; for example:

```
_storageGroup IN ["Default Storage Group"] _deviceGroup IN ["192.168.22.120 [TCPC]"] name="*[4924TestAlert]*" AND ("192.168.*" OR categoryBehavior CONTAINS Stop) | REGEX=":\d31" | cef name deviceEventCategory | chart _count by name
```

Additionally, a query can include constraints that limit the search to specific device groups and storage groups.

Logger offers several convenient ways to enter a search query:

- typing the query in the Search text box
- using Logger’s Search Builder tool to create a query, or
- using a previously saved query (referred to as filter or saved search)
- Retrieving saved searches and filters with “\$”, followed by its name

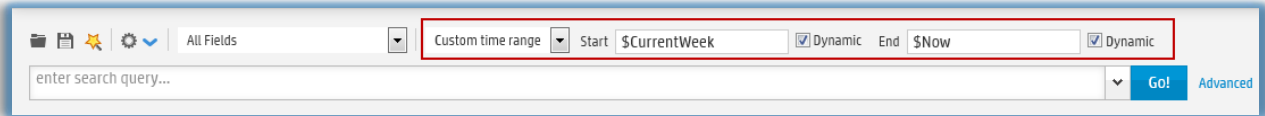
When you type a query, the auto-suggest facility in the user interface provides suggestions and possible matches for the fields you are entering and the applicable operators for those fields, thus enabling you to quickly build a query expression. The auto-suggest facility is available only for fields in the Logger schema, metadata terms (`_storageGroup`, `_deviceGroup`, `_peerLogger`), and the regular expression term (`|REGEX=`). Although a search query on Logger is as simple as entering a keyword to match, you will utilize the full potential of Logger’s search operation if you are familiar with all elements of a query, as described in the following section.

Building a Query



When you build a query, the following elements need to be specified:

- **Query Expression**—search conditions that are used to select or reject an event.
- **Time range**—the time range within which events should be searched.
- **Field Set**—fields of an event that should be displayed for matching events; for example, you can select to display only the deviceAddress and deviceReceiptTime fields of matching events.



Saving Queries for Later Use

If you need to run the same query regularly, you can save it in two ways:

- **Saved filter** - Save the query expression, but not the time range or field set information.
- **Saved search** - Save the query expression and the time range.

For more information about saving queries and using them again, see the Logger Administrator's Guide.

Query Building Tools


Logger offers the following tools to assist you in building queries that are complex:

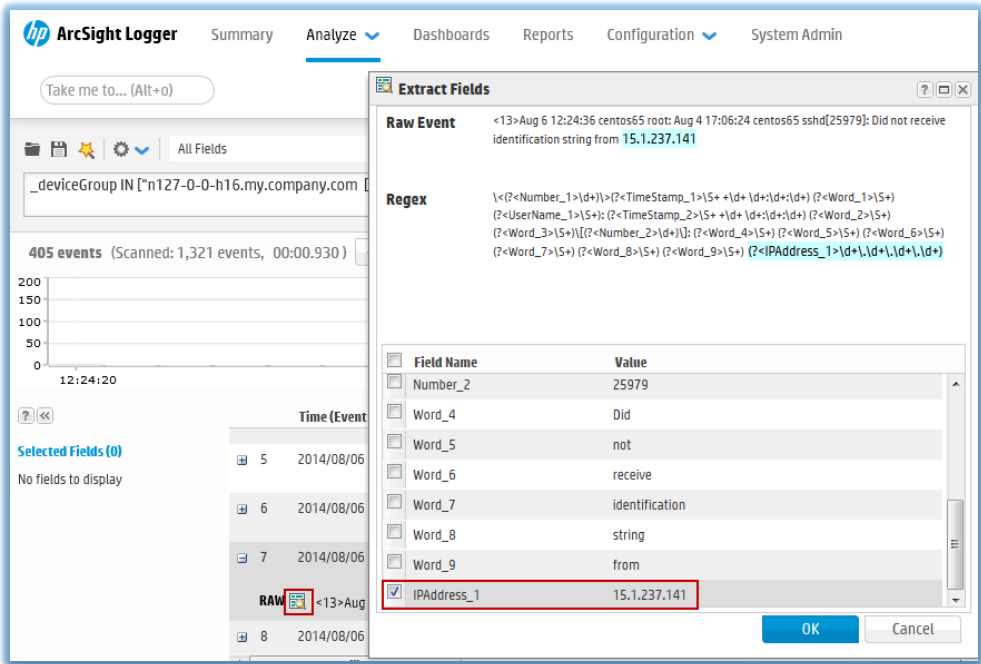
Search Builder

The Search Builder tool, as shown in the following figure, is a Boolean-logic conditions-editor that enables you to quickly and accurately build search queries. The tool provides a visual representation of the conditions you are including in a query. You can specify keywords, field-based conditions, and regular expressions using this tool. In addition, the tool enables you to specify search constraints such as device groups and storage groups.

Click Advanced Search below the Search text box to access this tool.

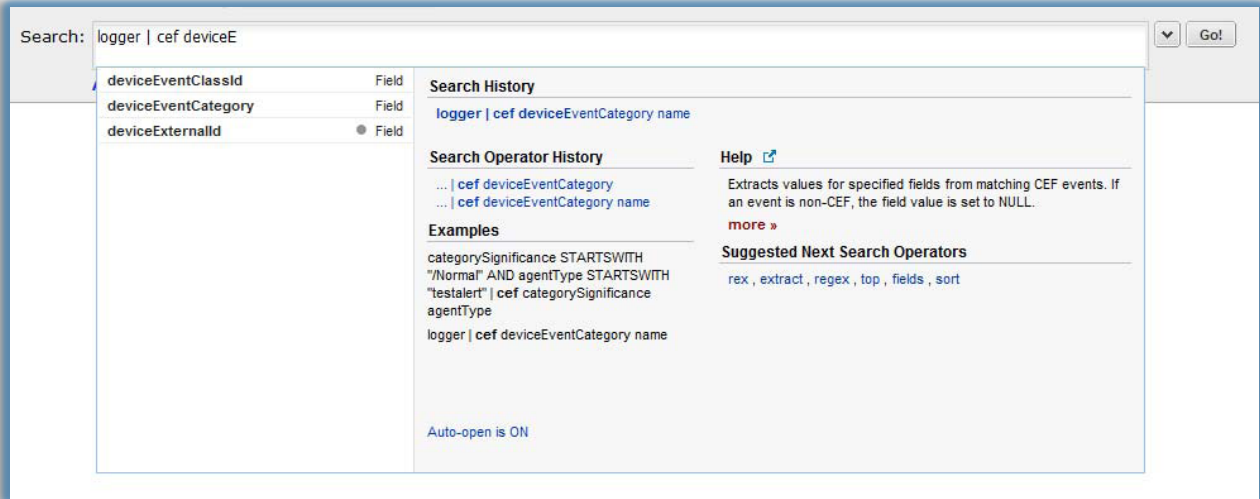
(For information about how to use this tool, see the Logger Administrator's Guide)

☐ **Regex HelperTool** 



The Regex Helper tool enables you to create regular expressions that can be used with the rex pipeline operator to extract fields of interest from an event. This tool not only simplifies the task of creating regular expressions for the rex operator but also makes it efficient and error-free. For details about this tool, see the Logger Administrator's Guide.

Search Helper



Search Helper is a search-specific utility that provides the following features:

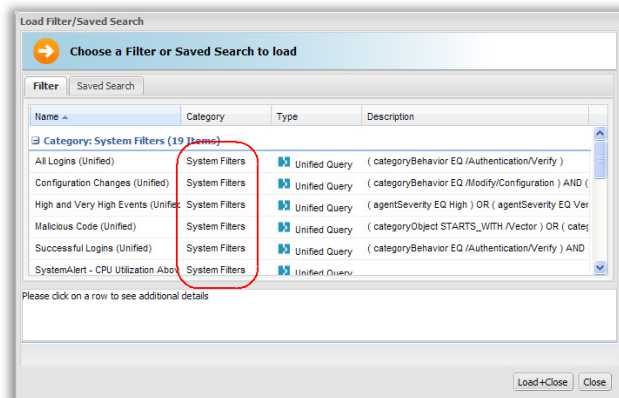
- **Search History**—Displays the recently run queries on Logger, thus enabling you to select and reuse previously run queries without typing them again.
- **Search Operator History** - Displays the fields used previously with the search operator that is currently typed in the Search text box.
- **Examples**—Lists examples relevant to the latest query operator you have typed in the Search text box.
- **Suggested Next Operators**—List of operators that generally follow the currently typed query. For example, if you type logger |, the operators that often follow are cef, rex, extract, or regex.
- **Help**—Provides context-sensitive help for the last-listed operator in the query that is currently typed in the Search text box.
- **List of Fields and Operators**—Depending on the current query in the Search text box, a complete list of fields that possibly match the field name you are typing or a list of operators that are available on Logger is displayed.

System Filters (Predefined Filters)

Your Logger ships with a number of predefined filters, also known as system filters. These filters define queries for commonly searched events. For example: unsuccessful login attempts or the number of events by source.

To use a system filter, follow the steps provided below:

1. Click **Analyze > Search**
2. Click the Load a Saved Filter icon (📁) to view a list of all system filters.



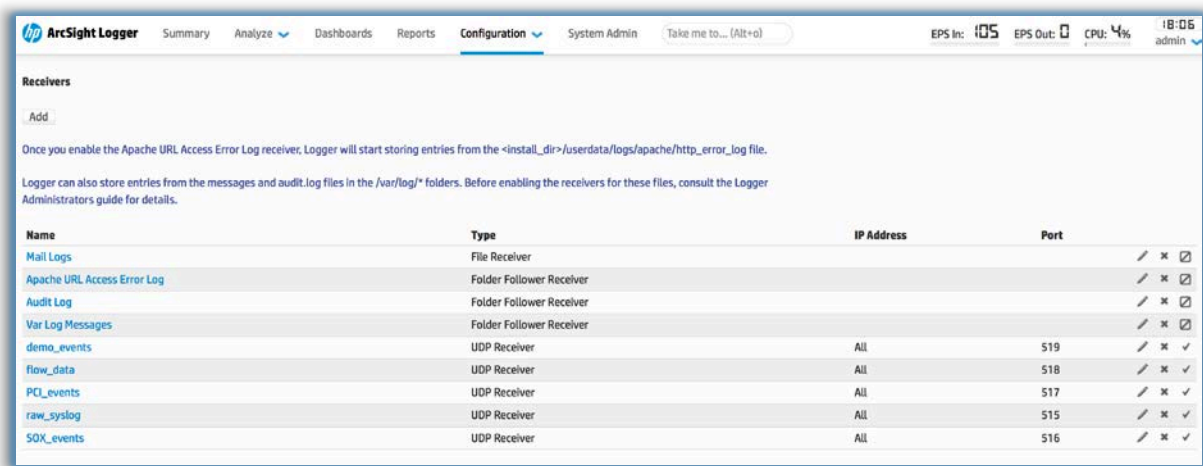
3. Click **Close**
4. Select **filter**
5. Click **Load+Close**.
6. Click **Go** to run the query.

7. Prepare System for Use Case Below

7.1. Configuring Logger to accept the Windows Unified Connector Events

Note: Some Logger Appliances have integrated connectors; other models require external Smart Connectors. Both require you to enable a receiver on the logger to receive the processed events.

From the Logger Menu, mouse over **Configuration**, under the **Data** column and select **Receivers** within the drop-down menu. Once at the devices page, Click the **“Add”** button.



Next, add a receiver with the the name of **“Windows”** and select **SmartMessage Receiver** from the available **type** options.

The 'Add Receiver' dialog box is shown. It has a title bar 'Add Receiver'. Below the title bar, there is a text input field for 'Name' containing the text 'Windows'. Below that is a dropdown menu for 'Type' with 'SmartMessage Receiver' selected. At the bottom of the dialog are two buttons: 'Next' and 'Cancel'.

Now, click **Next**

Edit Receiver

If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.

Name

Encoding

Source Type

Choose the default Encoding (**UTF-8**), a source type of **CEF** and choose **Save**



Note that the receiver is not enabled upon configuration

Click on the disabled symbol to enable the connector

Notice that the disabled symbol now shows a checkmark ✓ and the receiver is now enabled and ready to receive events.

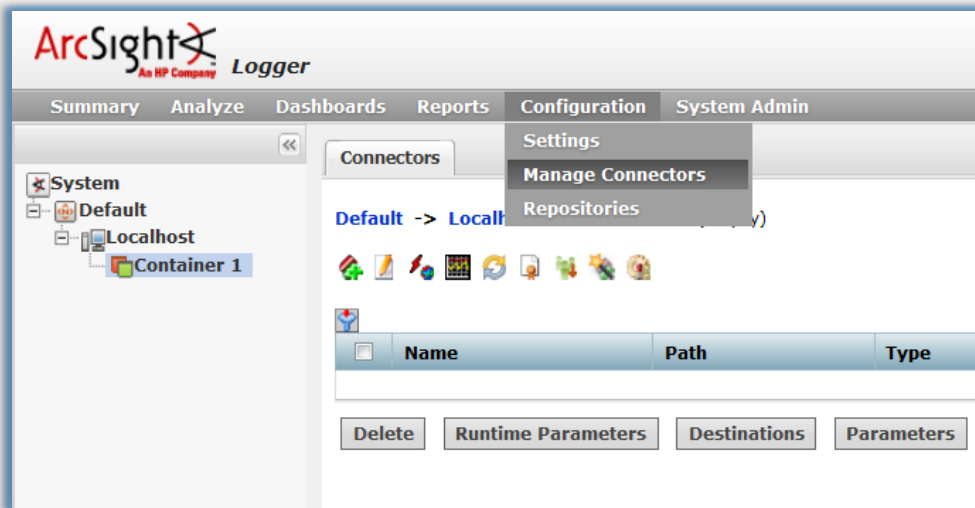



7.2. Configuring the Windows Unified Connector to collect and send events to a Logger appliance

Below are screenshots showing the general configuration of a Connector on a Connector Appliance. If you have the Software Logger [goto section 7.3](#)

If your logger supports onboard connectors:

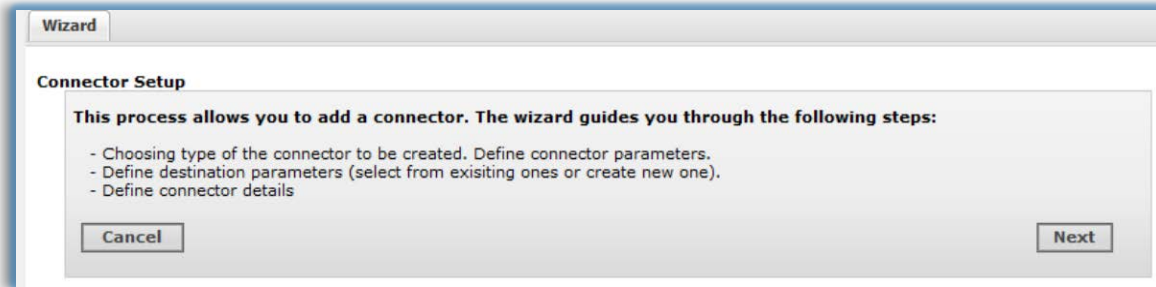
Choose **Configuration > Manage Connectors** to reveal the connector menus.



- 1) Click the add Connector icon () to start the process of adding a Connector.

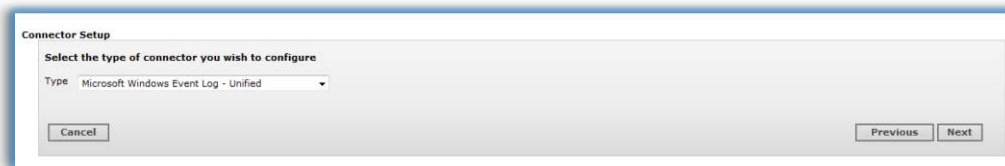


- 2) Click **Next**.

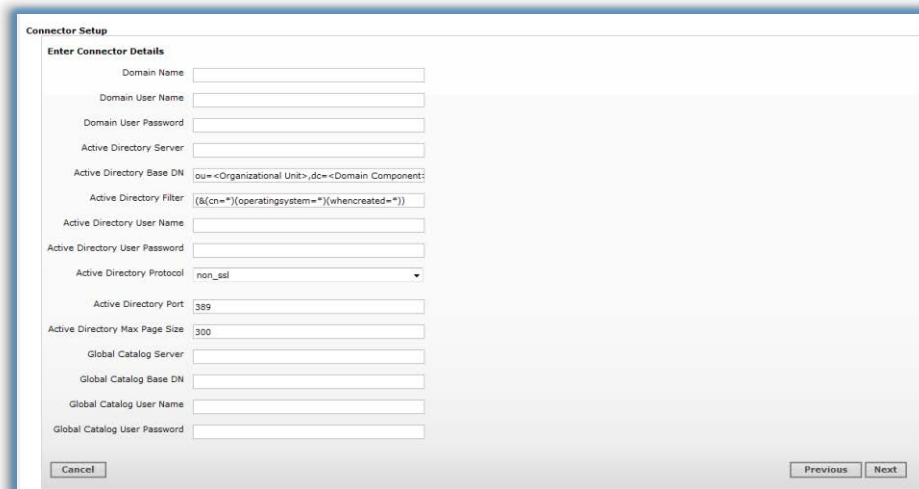


3) Choose the Connector Type you want to configure. This example chooses **“Microsoft Windows Event-Log-Unified”**

4) Run through the Connector Setup and choose **“Microsoft Windows Event Log – Unified”**

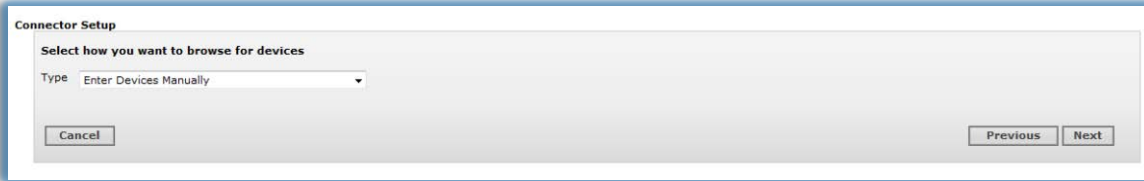


5) This next screen is only required if you will be using the Windows Host Browser. Since we will enter devices manually, you can skip this step and click Next.

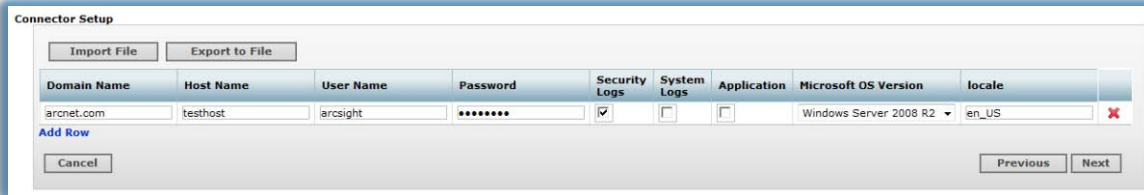


6) Choose to **“Enter Devices Manually”**





7) Click “**Add Row**” for each host that you want to collect events from.



Fill in the following parameters for each host you want to collect events from:

Domain Name - Name of the domain to which the host belongs. If you are using a Domain User account for a target host, fill in the Domain Name field. If you are using a Local User account for the target host, leave the Domain Name field blank. If the target host is a Workgroup host that does not belong to a domain, leave the Domain Name field blank.

Host Name - Host name or IP address of the target Windows host.

User Name - Name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain. Windows Server 2003 can utilize a standard domain user account. Windows 2008 servers can also utilize a standard Domain User Account and choose the new “Event Log Readers” built-in. See the [MicrosoftWindowsEventLogUnified.pdf](#) document for further details.

Password - Password for the user specified in User Name.

Security Logs - Select the check box for security events to be collected from this host; unselect the check box if you do not want to collect security events. The default value is checked (true)

System Logs - Select the check box for system events to be collected from this host; unselect the check box if you do not want to collect system events. The default value is unchecked (false)

Application - Select the check box for application events to be collected from this host; unselect the check box if you do not want to collect application events. The default value is unchecked (false)

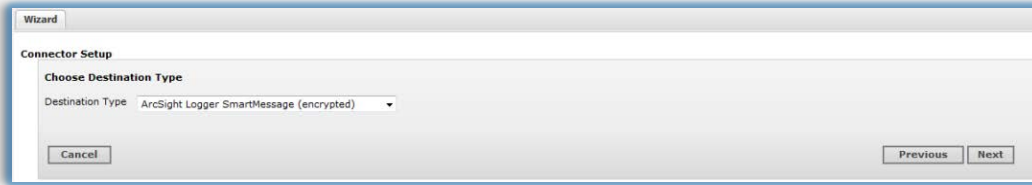
Microsoft OS Version - Select the Microsoft Operating System version this host is running.

locale - Enter the code for your locale; possible values are 'en_US' (United States English), 'ja_JP' (Japanese), 'zh_CN' (Simplified Chinese), 'zh_TW' (Traditional Chinese), 'fr_CA' (French). The default value is 'en_US'.

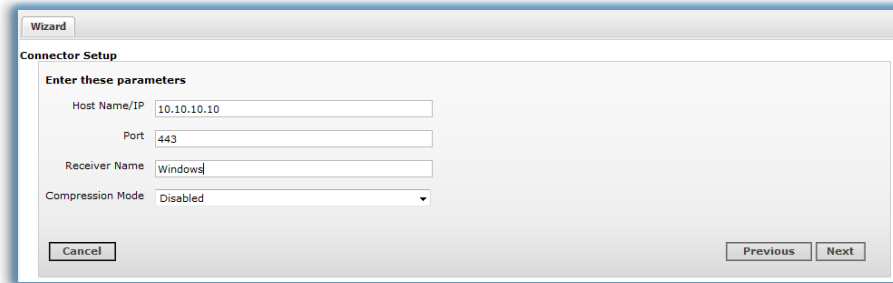
8) Click **Next** and continue on with the installation

9) Choose “**ArcSight Logger SmartMessage**” as the Destination Type.





10) Enter in the “**Hostname/IP**” of the Logger and the “**Receiver Name**” (note: A receiver should have already been created on the Logger). In our case the receiver is named “Windows”



7.3. Installing the Windows Unified Connector to collect and send events to a Software Logger

Obtain a current version of the ArcSight Smart Connectors.

For example if you download the Trial Logger you will have the following version

ArcSight-5.2.7.6544.0-Connector-Downloadable-Logger-Win.exe	Application	1/23/2013 4:49 PM	173,341,932	0%
-------------------------------------------------------------	-------------	-------------------	-------------	----

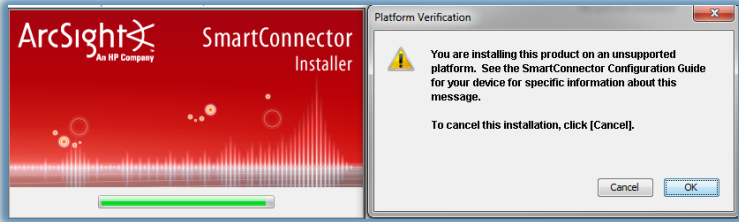
Or you may have the full version. As of this date the current version is 7.0.7

ArcSight-7.0.7.7279.0-Connector-Linux.bin	12/5/2014 4:16 PM	BIN File	171,445 KB
ArcSight-7.0.7.7279.0-Connector-Linux64.bin	12/5/2014 4:12 PM	BIN File	165,301 KB
ArcSight-7.0.7.7279.0-Connectors.aup	12/5/2014 4:08 PM	AUP File	584,383 KB
ArcSight-7.0.7.7279.0-Connector-Win.exe	12/9/2014 4:35 PM	Application	161,102 KB
ArcSight-7.0.7.7279.0-Connector-Win64.exe	12/5/2014 4:07 PM	Application	160,741 KB

As you can see there are multiple platforms that the connectors can be installed on.

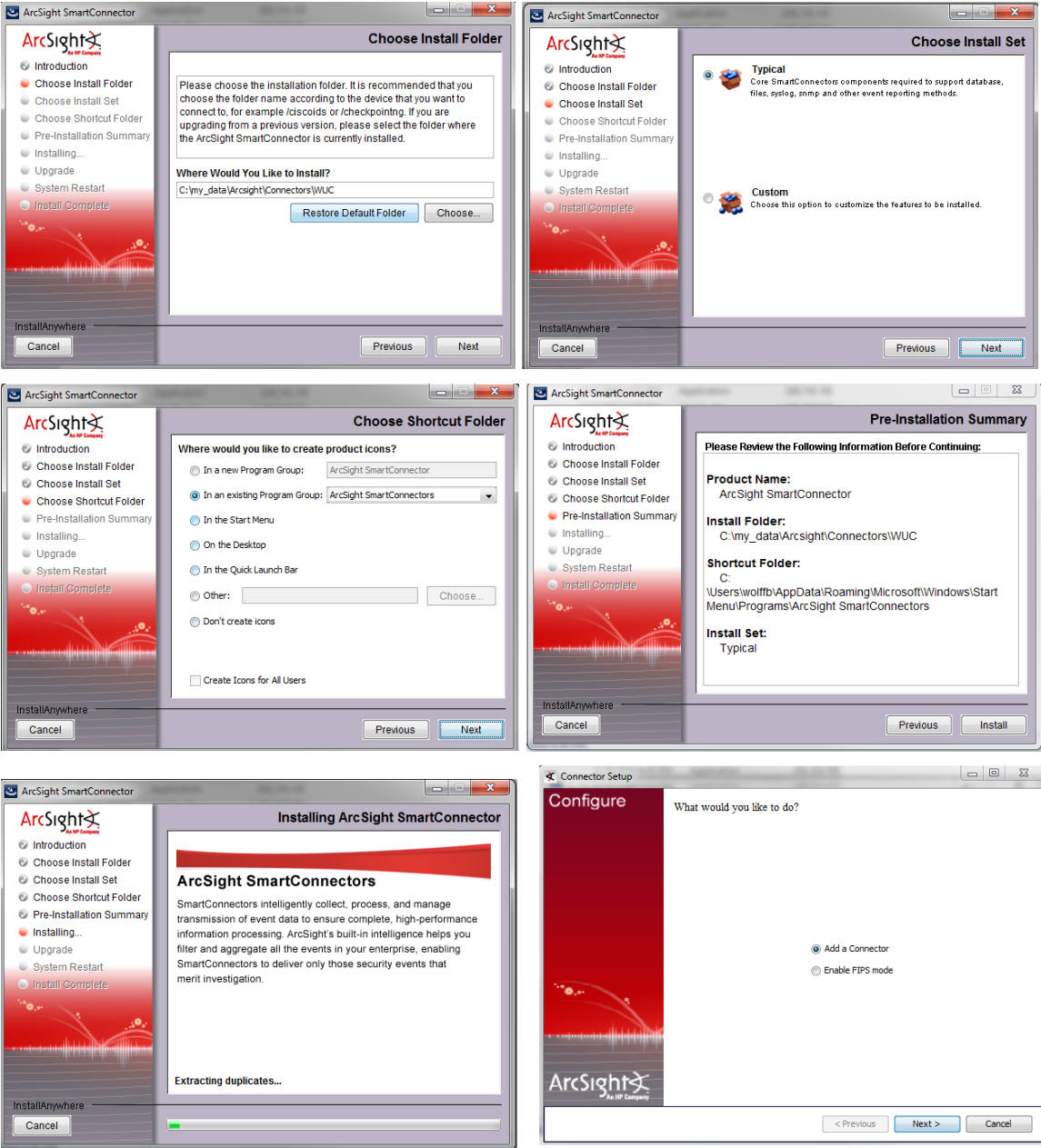
In this example I am installing the ArcSight-7.0.7.7279.0-Connector-Win.exe on Windows 7 workstation.

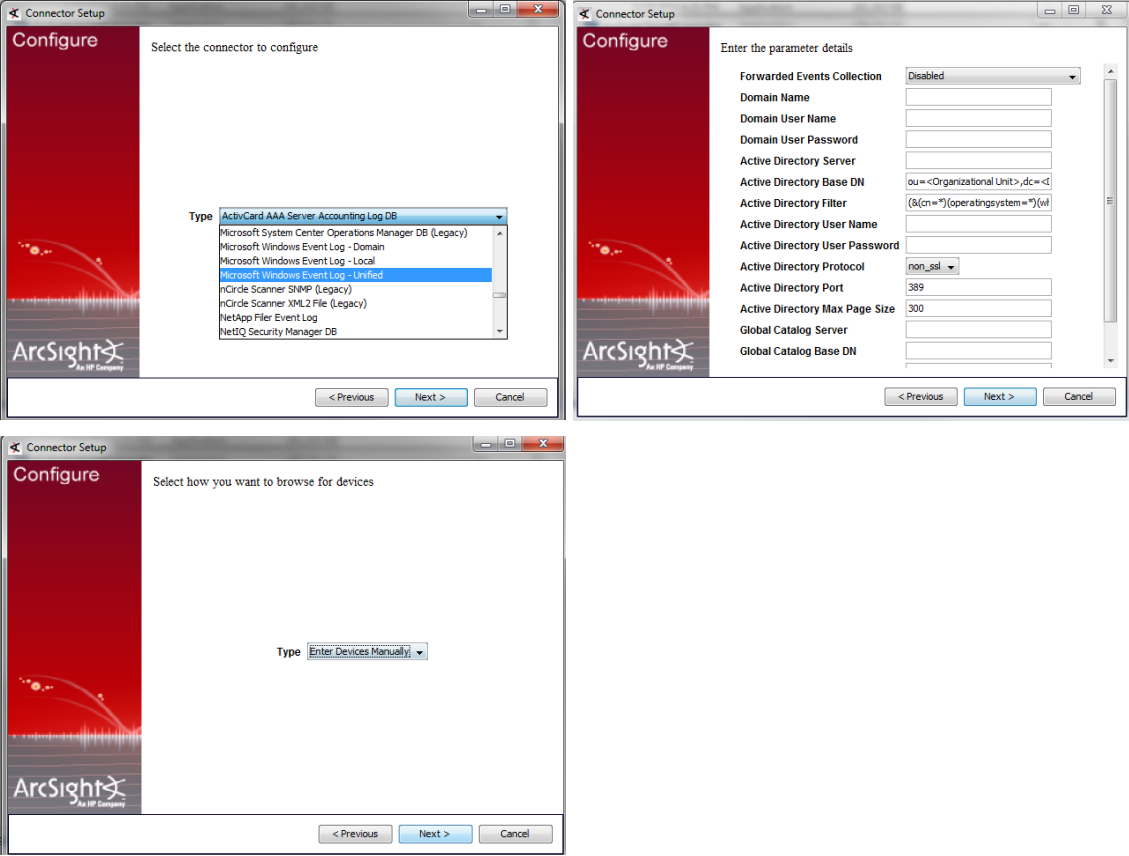




Just click OK to continue the installation.

In this case I choose to install the connector in C:\my_data\Arcsight\Connectors\WUC





TIP: Resize the screen for better view ability



Click Add, Enter the appropriate Values and click “Next”



If validation and logon to the device passes you will get the following screen, if not resolve the user/pass and domain entries as needed

Select ArcSight Logger SmartMessage (encrypted)



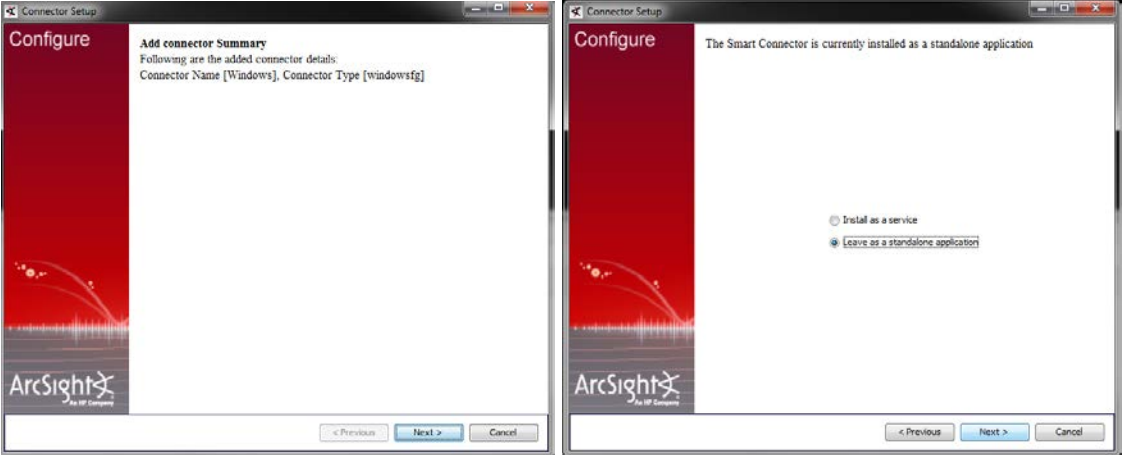
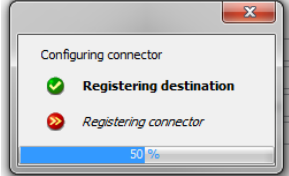
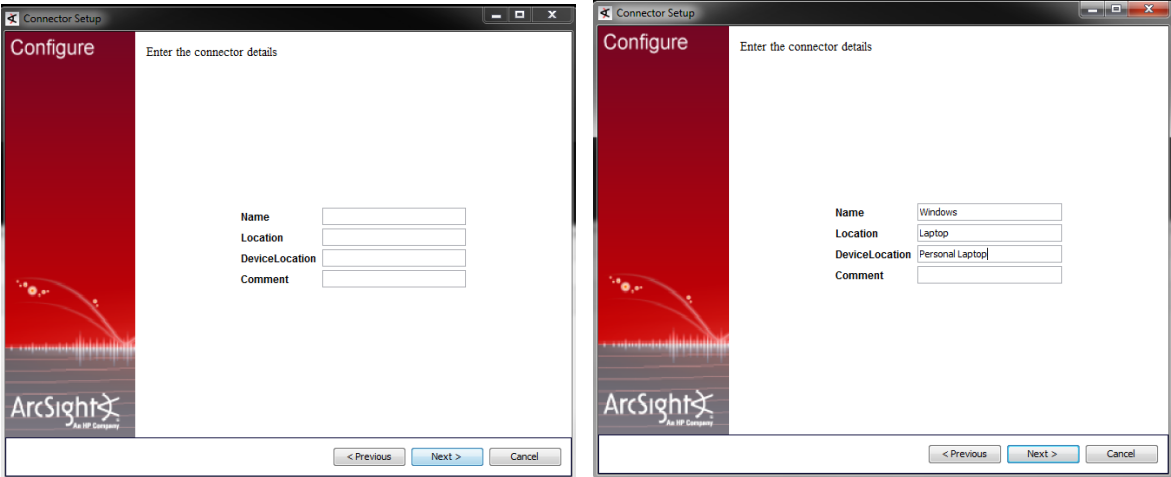


Next

Enter the hostname and receiver name

In my case the address is 172.16.100.100 and the Receiver Name was set to "Windows" which is case sensitive

You will get the following screen, if an error occurs follow the guidance given



Recommendation for testing is to leave as a standalone application, then once it is verified you can change it to a service.



Choose Next then Exit

Start a command window in windows

Change directory to C:\my_data\Arcsight\Connectors\WUC\current\bin where I installed the connector

```
C:\my_data\Arcsight\Connectors\WUC\current\bin>arcsight agents
```

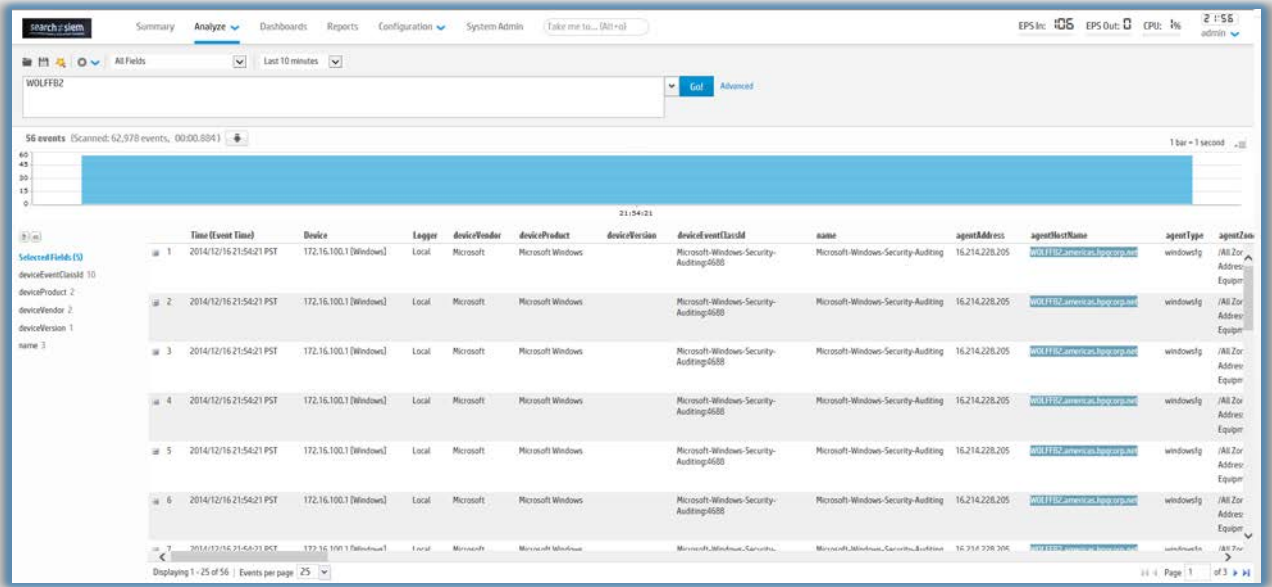
You will see something like the following

```
[Tue Dec 16 23:54:11 CST 2014] [INFO] Agent upgrade status check thread started  
[Tue Dec 16 23:54:11 CST 2014] [INFO] Device connection to [WOLFFB2] up. (Connected to Host)  
[Tue Dec 16 23:54:13 CST 2014] [INFO] First event from [ArcSight|ArcSight|16.214.228.205|wolffb2] received.  
[Tue Dec 16 23:54:13 CST 2014] [INFO] First event from [Microsoft|Microsoft Windows|!wolffb2.americas.hpqcorp.net] received.  
[GC 108817K->16403K(245760K), 0.0164244 secs]
```

Indicates the connector is up and the events are being sent to logger.

To confirm, go to the “Analyze” tab of the logger

Enter your machine name, in my case WOLFFB2



We can see that I received 56 events from the connector.



8. USE CASE Step by Step

We are interested in any activities surrounding **FAILED** logon attempts in Microsoft Windows

First we need to know how Microsoft Classifies Failed Logon Attempts

- 529 – Logon Failure – Unknown user name or bad password
- 530 – Logon Failure – Account logon time restriction violation
- 531 – Logon Failure – Account currently disabled
- 532 – Logon Failure – The specified user account has expired
- 533 – Logon Failure – User no allowed to logon at this computer
- 534 – Logon Failure – The user has not been granted the requested logon type at this machine
- 535 – Logon Failure – The specified account’s password had expired
- 536 – Logon Failure – The NetLogon component is not active
- 537 – Logon Failure –The logon attempt failed for other reasons.
- 538 – User Logoff
- 539 – Logon Failure
- 540 – Successful Network Logon

- 675 – Pre-authentication failed

Windows 2008R2

- 4624 – An account was successfully logged on
- 4625 – An account failed to logon
- 4634 – An account was logged off

As an administrator of Microsoft products you are already aware of the hundreds of codes that Microsoft uses to define their event codes. In this case we will conduct a simple text search for the entry “**Security:529**” or for Windows 2008 “**Microsoft-Windows-Security-Auditing:4625**”

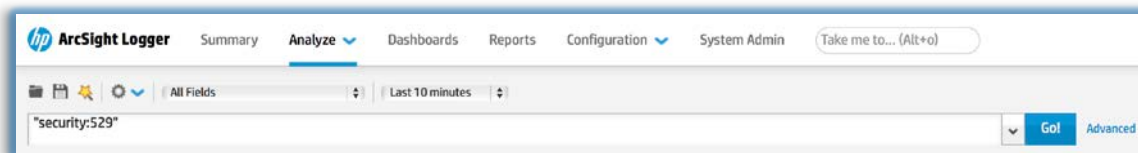
Thankfully ArcSight recognizes that not everyone is an expert in security codes for dozens of products and uses categorization to eliminate the need to know specific codes.

Read more about Categorization in section 7.2 below.

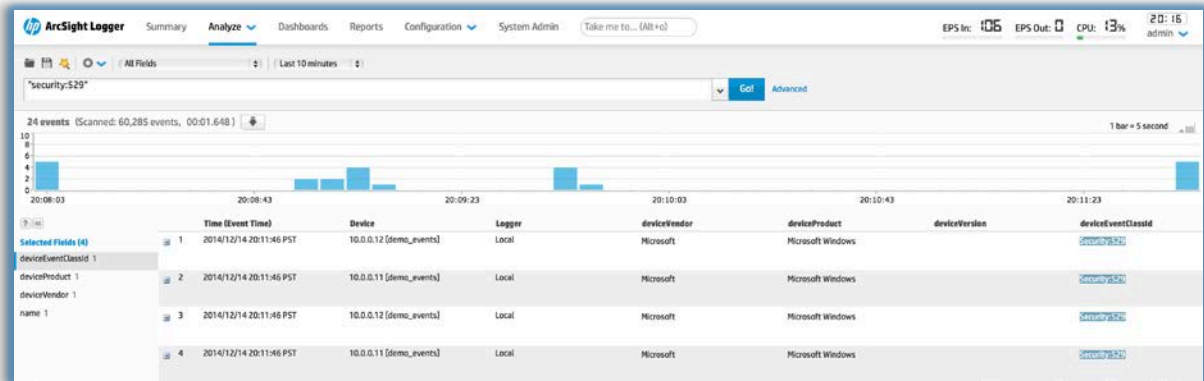
8.1. Search / Analyze

Mouse over “**Analyze**”, and select “**Search**” from the menu

And in the Search area enter: “*Security:529*” OR
for Windows 2008:”*Microsoft-Windows-Security-Auditing:4625*”

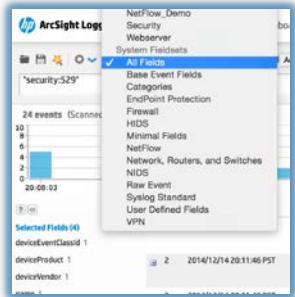


As you can see the events that meet the query have been returned and are displayed for further revision and/or analysis.



You can change the presentation of the results by choosing or creating a display set in the Fields: portion.

To change the Field set click the Select the "Categories" field



drop down box next to "Fields:" set.

The screenshot shows the event results table with several columns circled in green. The table contains the following data:

Time (Event Time)	Device	Logger	deviceEventClassId	name	deviceVendor	deviceProduct	categoryBehavior	categoryDeviceGroup
1 2014/12/14 20:11:46 PST	10.0.0.12 [demo_events]	Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
2 2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
3 2014/12/14 20:11:46 PST	10.0.0.12 [demo_events]	Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
4 2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
5 2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System

Minimize the Field Summary at this time by clicking on the [button] We will discuss this shortly



8.2. Categorization

As you can see the **Security:529** has been returned but I am now focusing on the fields related to categorization. First notice that the **Security:529** appears under the field name **deviceEventClassId**.

ArcSight SmartConnectors normalize, categorize and prioritize all events as they are being obtained from the logging systems. This eliminates the need to understand each vendor's individual coding of events and allows you to use categorization to find the nature of the information you are looking for.

As you can see **Security:529** is categorized as:

categoryBehaviour /Authentication/Verify
categoryDeviceGroup/Operating System
CategoryObject /Host/Operating System
CategoryOutcome /Failure
CategorySignificance /Information/Warning

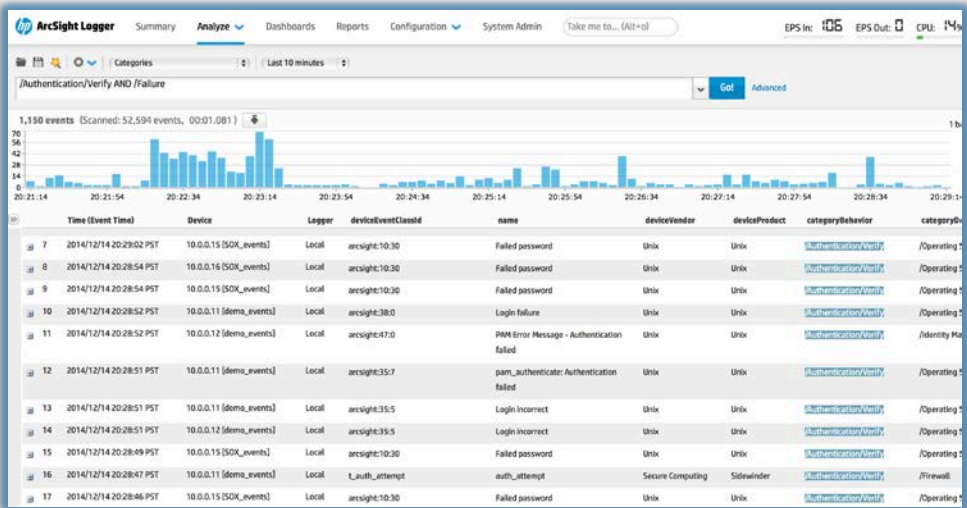
For Windows 2008 you see that **Microsoft-Windows-Security-Auditing:4625** is categorized in exactly the same way

Logger	deviceEventClassId	name	deviceVendor	deviceProduct	categoryBehaviour	categoryDeviceGroup	categoryObject
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System

Now modify the search and look for /Authentication/Verify AND /Failure instead.

Delete "Security:529 " from the Search area and replace with:
"/Authentication/Verify and /Failure" and click "Go"



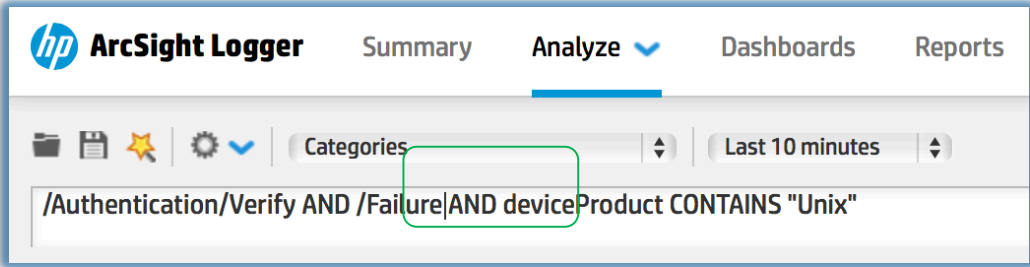


Instead of being limited to Authentication Failures specific to Microsoft, I now see ALL events classified as Authentication Failures regardless of Vendor. Here we see UNIX and Sidewinder. Notice that any time the search criteria are met, the display highlights that entry for fast location visually.

By hovering over an entry, in this case “Unix” all matching events are highlighted.

Time (Event Time)	Device	Logger	deviceEventClassId	name	deviceVendor	deviceProduct	categoryBehavior	categoryD
2014/12/14 20:28:52 PST	10.0.0.12 [demo_events]	Local	arcsight:47:0	PAM Error Message - Authentication failed	Unix	Unix	/Authentication/Verify	/Identity Management/AAA
2014/12/14 20:28:51 PST	10.0.0.11 [demo_events]	Local	arcsight:35:7	pam_authenticate: Authentication failed	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:51 PST	10.0.0.11 [demo_events]	Local	arcsight:35:5	Login Incorrect	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:51 PST	10.0.0.12 [demo_events]	Local	arcsight:35:5	Login Incorrect	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:49 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:47 PST	10.0.0.11 [demo_events]	Local	t_auth_attempt	auth_attempt	Secure Computing	Sidewinder	/Authentication/Verify	/Firewall
2014/12/14 20:28:46 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:44 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:40 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Verify	/Operating System
2014/12/14 20:28:39 PST	10.0.0.11 [demo_events]	Local	Failed Login Attempt	Failed Login Attempt	Nortel	VPN	/Authentication/Verify	/VPN

If you click “UNIX” under deviceProduct column, the search is modified. Note that we are now adding a Structured Search Element to the free form text search. The normalized column name now appears in the search. If instead you choose ALT-Click you can automatically insert a NOT condition into the search string.

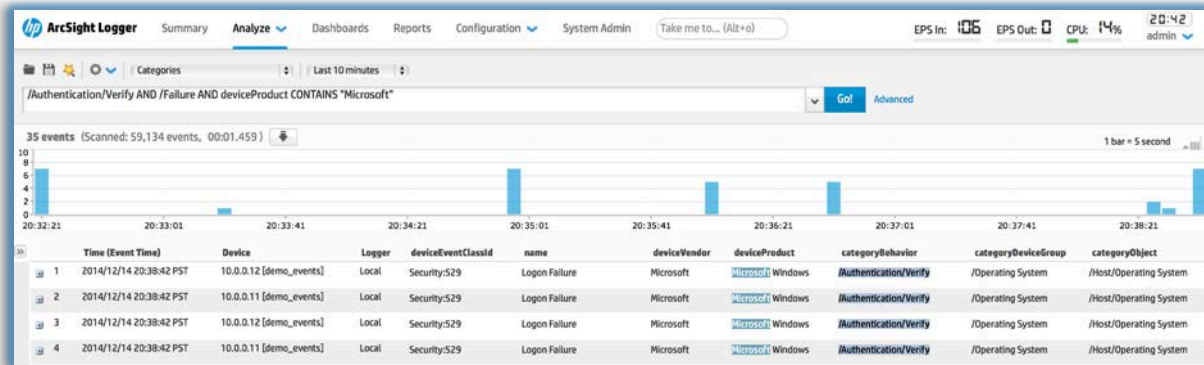



This narrows the previous search further to only those events that contain Unix as the deviceProduct. Let’s change our focus back to Microsoft Events, by replacing “Unix” with “Microsoft” in the Search Area.

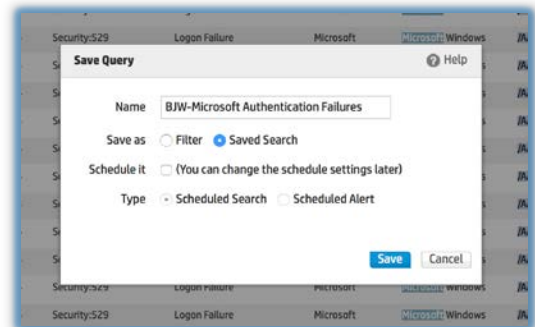
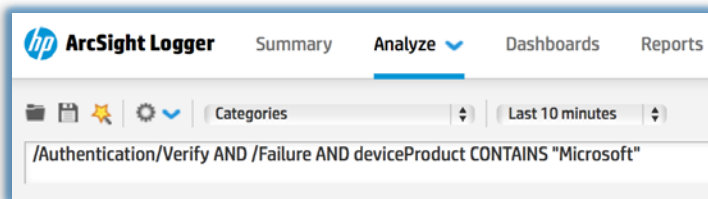


Your entry should look like this:

/Authentication/Verify and /Failure AND deviceProduct CONTAINS "Microsoft"



At this point I want to save this query for future use. Press the  to save the search.



Give it the name "**Microsoft Authentication Failures**"

My suggestion is to personalize your Saved Queries by adding your initials to the description.


Click the "**Saved Search**" radio button to the right of "Save as"

Click **Save**

Field Summary

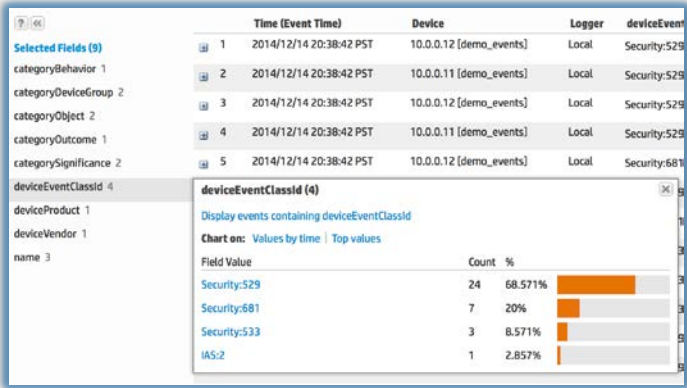
You have noticed the field summary in the past, but let us explore what it does.

You can rapidly find additional information about the events returned without having to manually count the items you are interested in.

Expand the Field Summary window by clicking on the arrow  For the Field Summary Window

Click on **deviceEventClassId** in the Field Summary

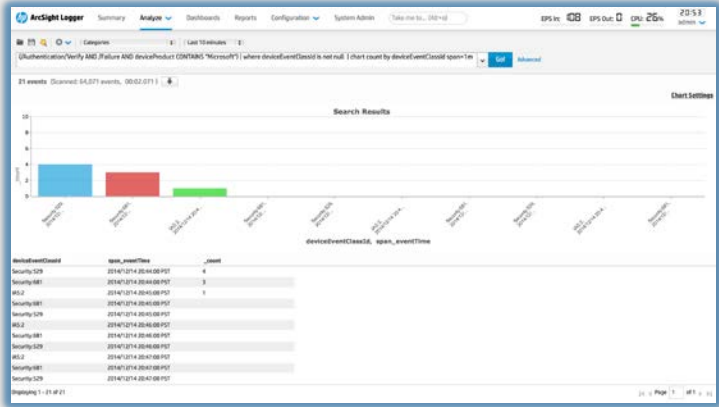
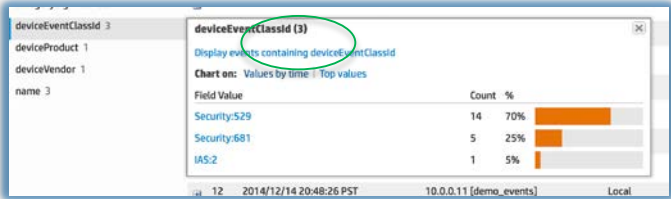




Notice that we have 4 different values that appear in our return set. These statistics help me focus on the information I am interested in.

Say I am only interested in Security:533, just click on that value. As you would expect the query was automatically changed to: **(/Authentication/Verify and /Failure AND deviceProduct CONTAINS "Microsoft") and deviceEventClassId = "Security:533"**

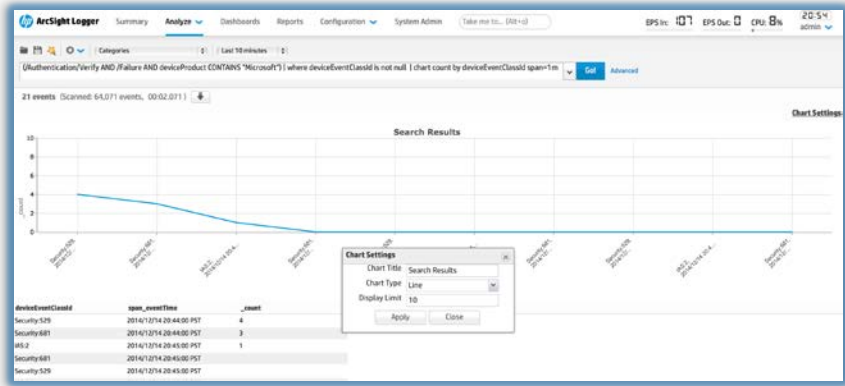
Delete the addition "and deviceEventClassId = "Security:533" to get to our original query and click on deviceEventClassId again. This time choose "Values by time"




As you can see the system quickly created a chart by time for further interpretation.

However for better interpretation, click on "Chart Settings" and Choose "Line"





Now let's restore our save search by clicking on the  icon. Choose the "Saved Search Tab"

The screenshot shows the "Load Filter/Saved Search" dialog box. It has two tabs: "Filter" and "Saved Search". The "Saved Search" tab is active, displaying a table of saved searches:

Name	Type	Start Date	Start Time	End Date	End Time	Local
BJW-Microsoft Authentication Failures	Unified Query	\$Now - 10m		\$Now		
BJW-Microsoft Authentication Failures	Unified Query	\$Now - 10m		\$Now		
Configuration - Configuration Changes (chart)	Unified Query	\$Now - 10m		\$Now		
Configuration - Configuration Changes (chart) [Import]	Unified Query	\$Now - 10m		\$Now		
Configuration Changes by Product	Unified Query	\$Now-1h		\$Now		<input checked="" type="checkbox"/>
Demo NetFlow by port	Unified Query	\$Now - 10m		\$Now		

Below the table, the selected search details are shown:

Name: BJW-Microsoft Authentication Failures
Type: Unified Query
Description: /Authentication/Verify AND /Failure AND deviceProduct CONTAINS "Microsoft"

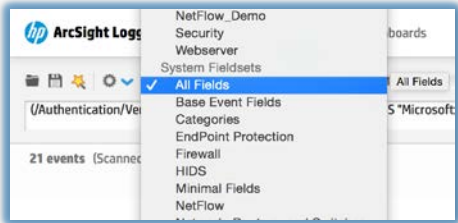
At the bottom right, there are buttons for "Load + Close" and "Close".

Click on "Load + Close", then click on "Go" to execute the query



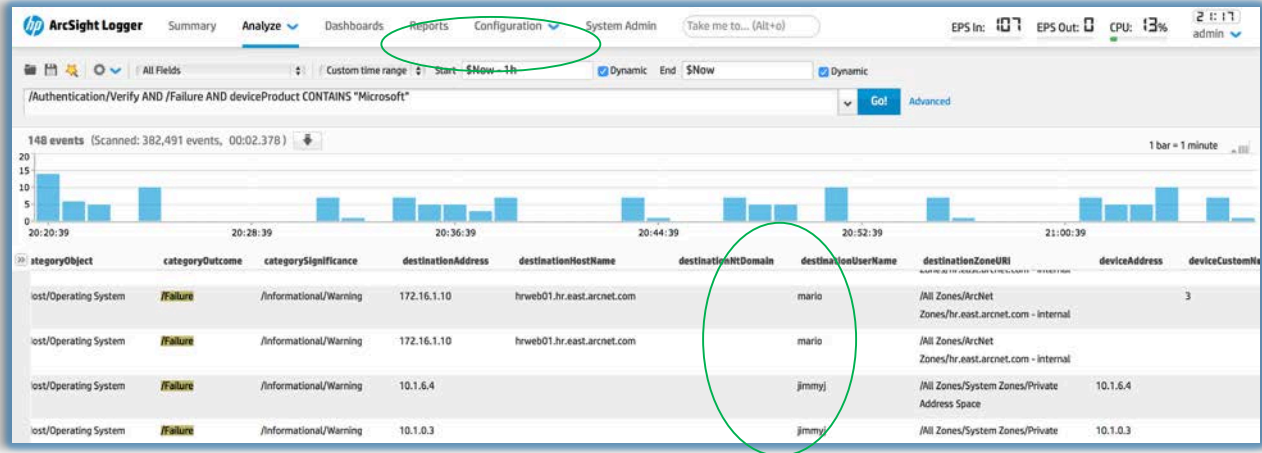
Fields

Change the field display and set it back to “All Fields”

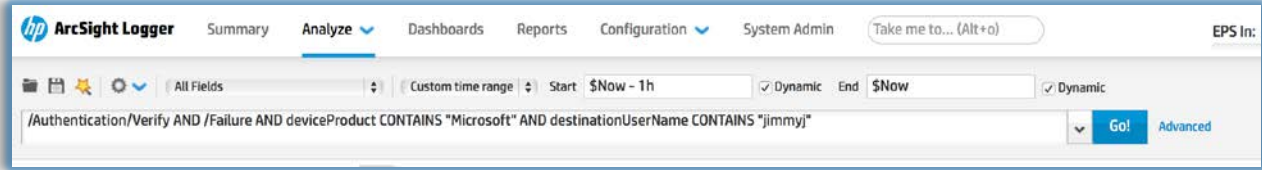


Now scroll to the right to see the **destinationUserName** field.

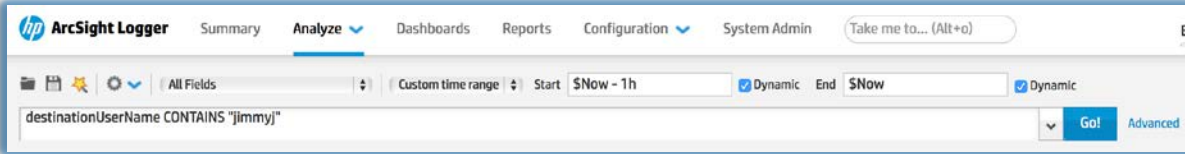
Ensure the Start Time is set to “\$Now – 1h”



Now let’s click on a user, in my case “jimmyj”




Now I want to see all activity related to this user ID by deleting all criteria prior to destinationUserName. Your search should be destinationUserName CONTAINS "jimmyj"

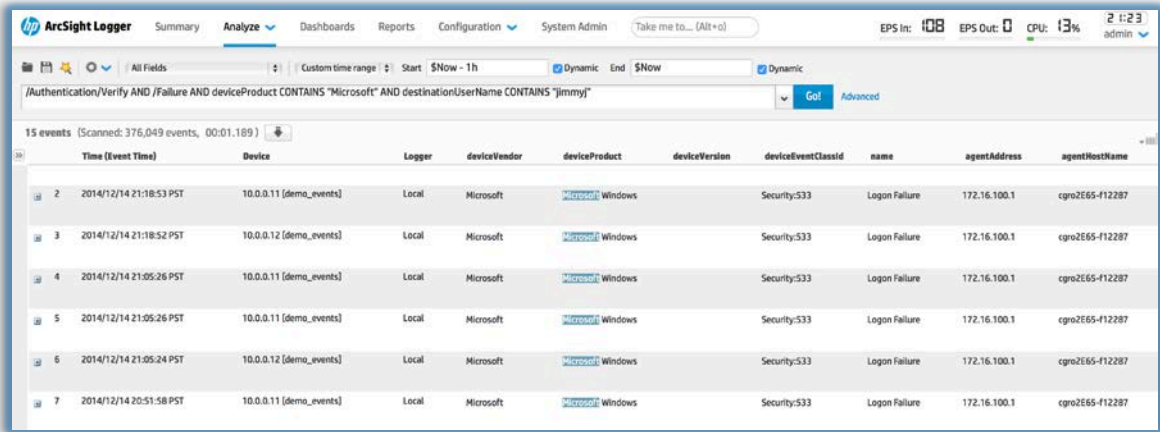


Minimize the “Radar” by clicking on the up-arrow in the following

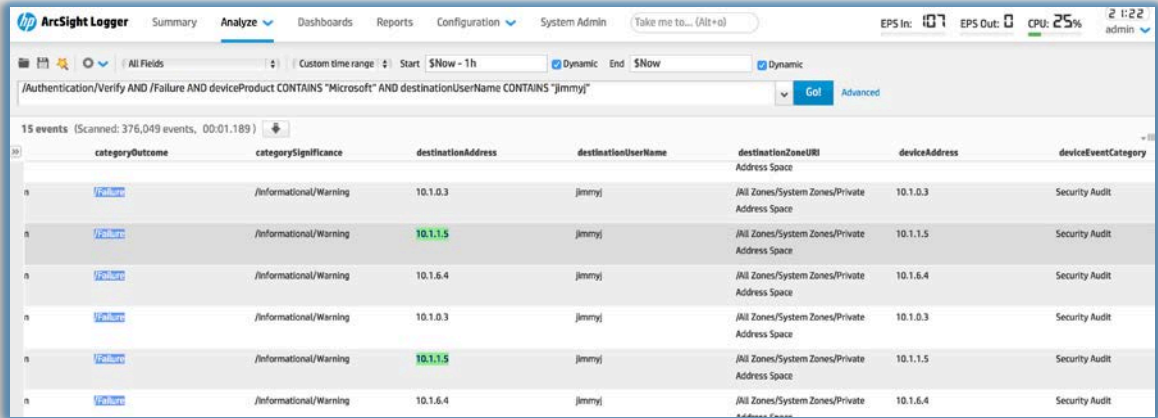


1 bar = 1 minute 

Minimize the “Field Summary” by clicking on 



Notice that “jimmyj” only appears in Microsoft events at this point so let’s change the investigation to view activity based on an IP address instead. Click on an IP in the **deviceAddress** field.



Then remove the search for jimmyj so it looks like this.

destinationAddress CONTAINS "10.1.1.5"

Now you can see activity from all of the feeds where the **deviceAddress** contains **10.1.1.5** for example Tripwire, Microsoft, Oracle and others. (depends of course on your event feeds)

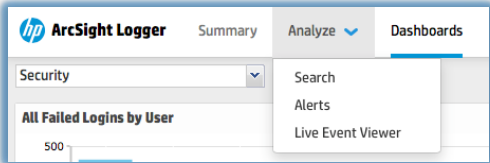


address	agentHostName	agentZoneURI	baseEventCount	categoryBehavior	categoryDeviceGroup	categoryObject	categoryOutcome	categorySignificance	destinationAddress	destinationDomain
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Modify/Content	/Operating System	/Host/Resource/File	/Success	/Informational	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/Informational/Warning	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/Informational/Warning	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/Informational/Warning	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/Informational/Warning	10.1.1.5	

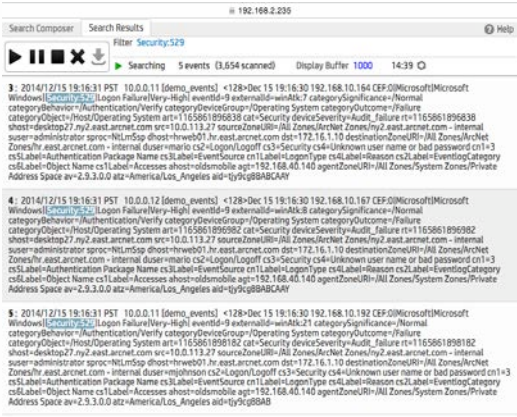
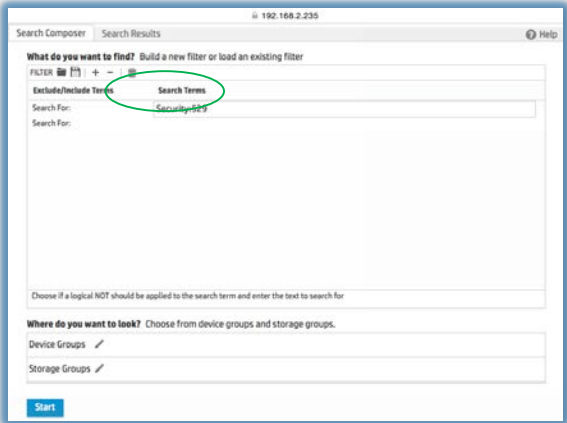
8.3. Viewing a Live Feed

Many individuals prefer to see events that are a constant scroll by like a “tail –f” command in UNIX. We have this capability thru the Live Event Viewer

Choose Analyze > Live Event Viewer



Enter “Security:529” in the top “Search For” box



8.4. Dashboards

8.4.1. Data Monitor: MS - Last Logon Failures

Now I want to create a Data Monitor that will show me the last 10 windows logon failures.

categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure" AND NOT (destinationUserName IS NULL) | top destinationUserName

Or we can also limit our analysis to Microsoft only failures by adding before the | top destinationUserName

"AND deviceProduct CONTAINS "Microsoft"

Example:

categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure" AND NOT (destinationUserName IS NULL) AND deviceProduct CONTAINS "Microsoft" | top destinationUserName

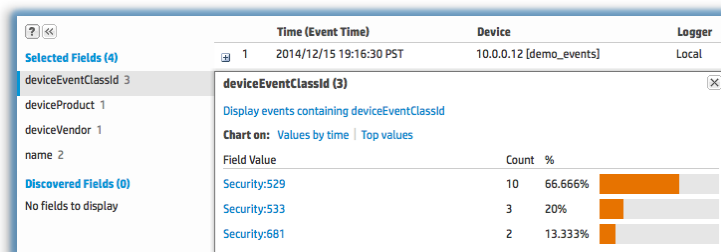
By viewing the Field Summary we can quickly see the percentages of each deviceEventClassId that is in the return data set.

(NOTE- when displaying the chart "| top destinationUserName" I do not get the Field Summary option

You can choose to chart the "Values by Time" or "Top Values" by clicking on the appropriate label.

Enter the search in the search box:

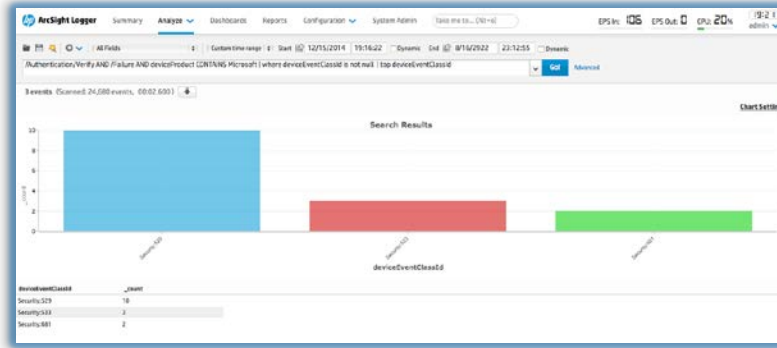
/Authentication/Verify AND /Failure AND deviceProduct CONTAINS Microsoft



Click on **"Top values"**

Notice that a chart is automatically built for you





Since this is my area of responsibility I want to place this in a dashboard so that I can quickly see the current results without having to execute a search this time.

Now I want to save this chart so I can use it in a dashboard. Click on 

Notice that there is a new choice presented. Dashboard Panel. Click on **Dashboard Panel**

The 'Save Query' dialog box has the following fields and options:
Name: Microsoft Authentication Failures
Save as: Filter Saved Search Dashboard panel
Schedule it: (You can change the schedule settings later)
Type: Scheduled Search Scheduled Alert
Buttons: Save, Cancel

The 'Save Query' dialog box has the following fields and options:
Panel Title: Microsoft Authentication Failures
Save as: Filter Saved Search Dashboard panel
Saved Search: New saved search
Saved search name: [empty field]
 BJW-Microsoft Authentication Failures
Dashboard: Mail
 New dashboard
Dashboard name: Microsoft Related Events
Panel type: Chart Add both types
Chart type: Pie
Chart limit: 10
Buttons: Save, Cancel

Notice the choices made:

Select Saved search as “Microsoft Authentication Failures” reusing the query

Select “New dashboard” and enter “Microsoft Related Events”

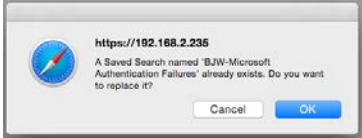
Checkmark “Add both types”

Change Chart type to “Pie”

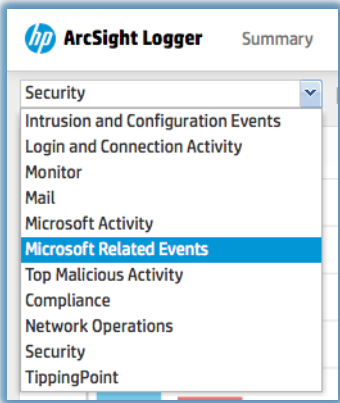
Click on Save

The following message will pop up:





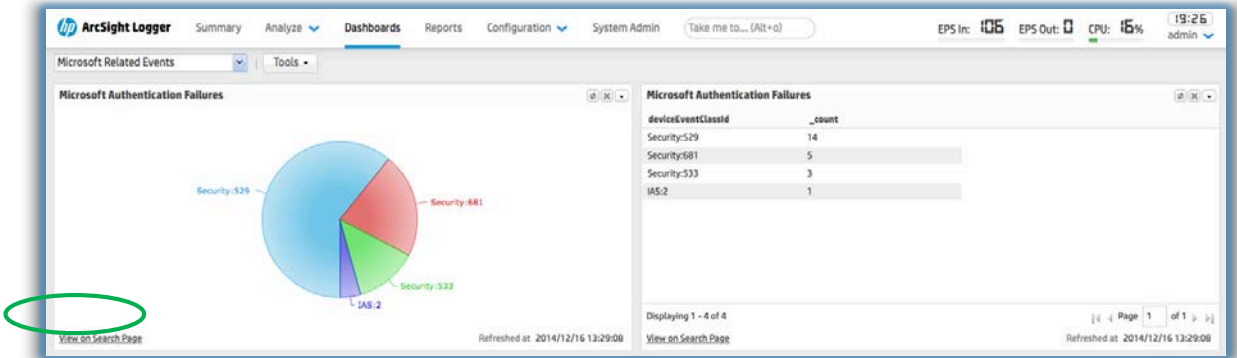
Choose **OK**



Click on **Dashboards**

Change drop down to **"Microsoft Related Events"**

Your dashboard is now displayed.



Let's add another dashboard by building on what the system already created for us.

Click on **"View on Search Page"** The system jumps to the Analyze Tab and displays `/Authentication/Verify and /Failure AND deviceProduct CONTAINS Microsoft | where deviceEventClassId is not null | top deviceEventClassId`

Change this to:

`/Authentication/Verify and /Failure AND deviceProduct CONTAINS Microsoft | top destinationUserName`

You have probably already noticed that the system has extensive context sensitive help prompting you and giving you examples every step of the way.

Click on **GO**



hp ArcSight Logger Summary Analyze Dashboards Reports Configuration System Admin Take me to... (Alt+o)

Custom time range Start 12/15/2014 19:16:22 End 8/16/2922 23:12:55

/Authentication/Verify AND /Failure AND deviceProduct CONTAINS Microsoft | top destinationUserName

Search History
/Authentication/Verify AND /Failure AND deviceProduct CONTAINS Microsoft | top destinationUserName

Search Operator History
... | top destinationUserName

Examples
arcsight | cef deviceEventCategory | top deviceEventCategory
_storageGroup IN ["Default Storage Group"] | cef deviceEventCategory
eventid | rex "deviceEventCategory=?<categories>[*]" | top categories

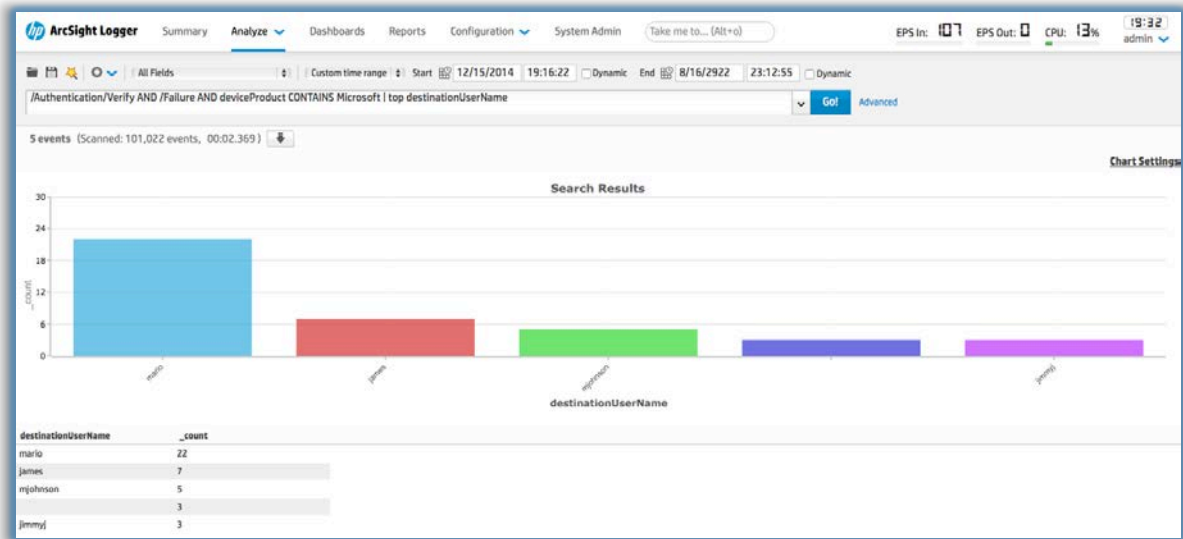
Help
List the search results in a tabular form of the most common values for the specified field. That is, the values are listed from the highest count value to the lowest.

Usage
| top [<n>] field1 field2 field3 ...
<n> limits the matches to the top n values for the specified fields.
more »

Suggested Next Search Operators
chart , fields , sort , rex , where

Auto-open is ON

destinationUserName



Change to a Pie Chart

Chart Settings

Chart Title: Search Results

Chart Type: **Column**

Display Limit: Column

Apply

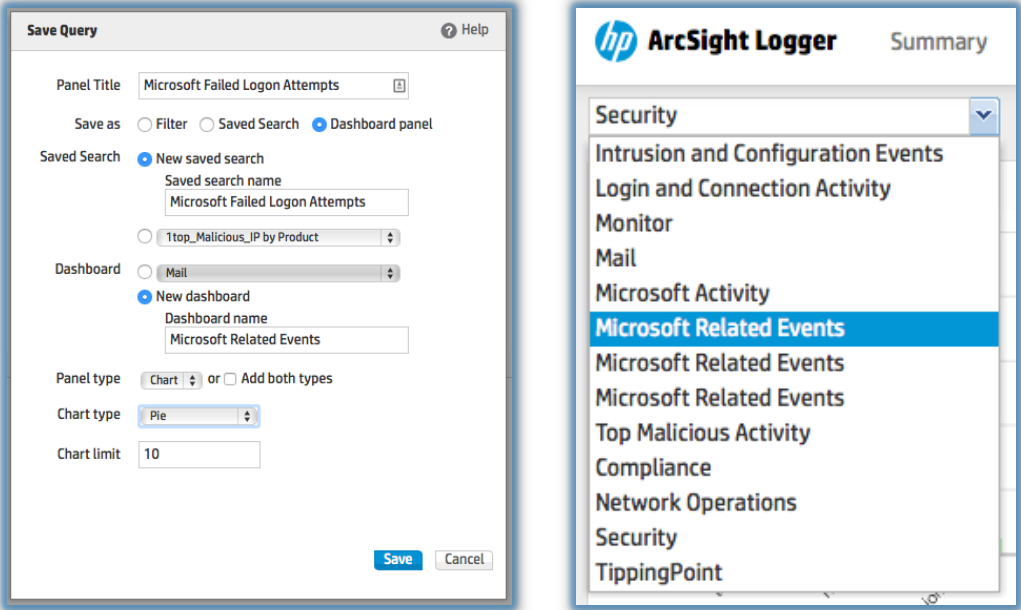
Close

- Column
- Bar
- Pie**
- Area
- Line
- Stacked Column
- Stacked Bar

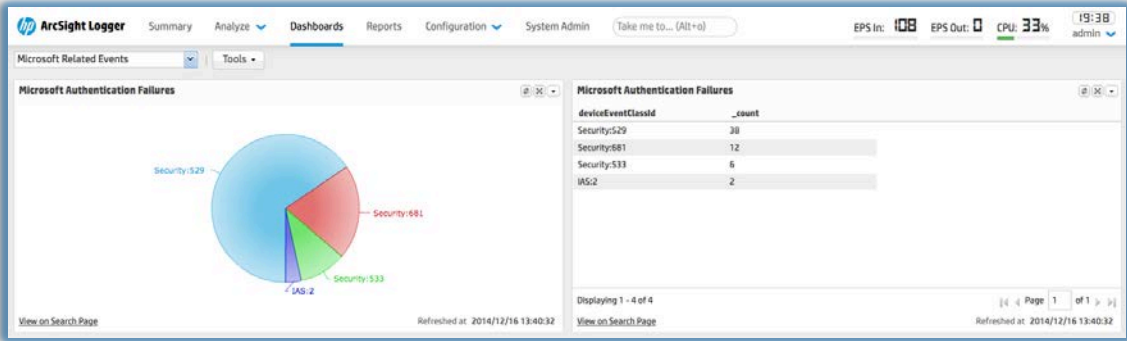
Choose **SAVE**



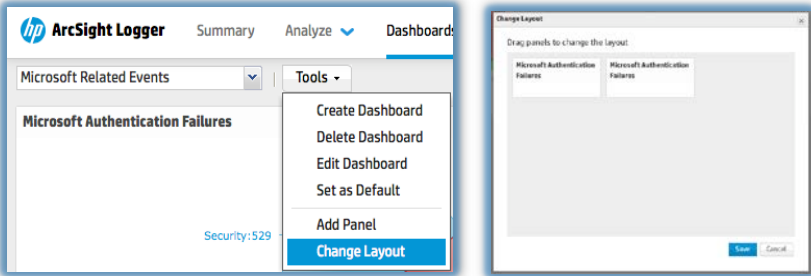
Enter the selections as shown below and click **SAVE**



Select the “Dashboards” tab and “Microsoft Related Events” from the dropdown box on the right.



Change the format of the display
Click on Tools and choose Change Layout



Choose Save



8.5. Reporting

[Dashboard Viewer](#) [Dashboard Preferences](#) [Widget Designer](#) [Recent Reports](#) [Jobs Execution Status](#) [Classic Viewer](#) [Classic Designer](#) [Classic Preferences](#)

When you choose “Reports from the menu or the “Take me to...” dialogue, you will be brought to the Dashboard Viewer. Dashboards display reporting data to provide a quick view of the latest information about network events. You can assemble various reports and external links onto a dashboard.

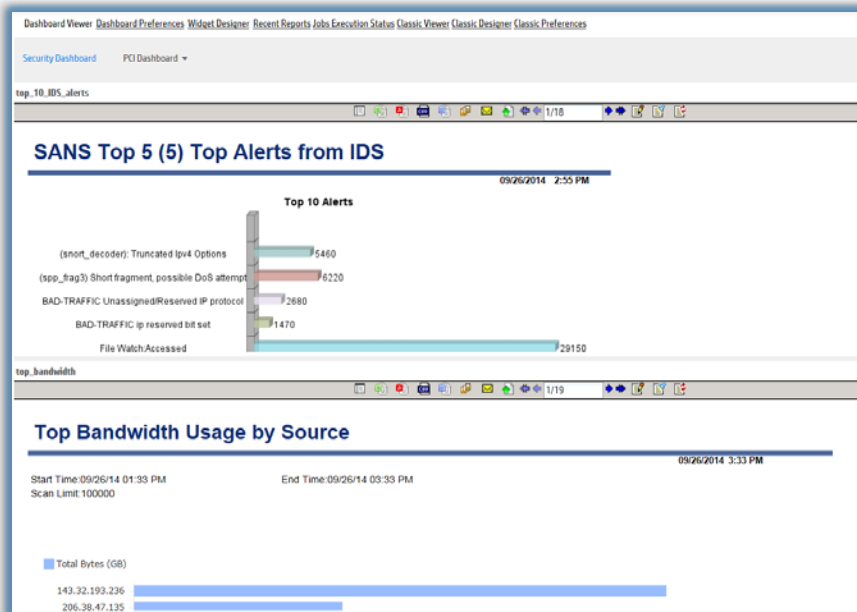
However, you must place each report or link into its own widget and then place the widget in the dashboard. A dashboard can contain multiple widgets.

Placing reports on a dashboard gives you access to the most recently published results for those reports. Keep in mind, reports must be run and published in order for the results to be accessible on a dashboard viewer. If you schedule a report to run, publish, and save for a reasonable retention period (for example, one month), then those results will always be available for dashboard views.

For example, you can add one or more reports to a dashboard, and configure reports to auto-refresh on a specified interval (for example, every hour). The dashboard will access the latest published reports results, in this case, every hour.

If you have also scheduled the reports to run and publish every hour, your dashboard will show current results. This eliminates the need to manually run and view each report once per hour in order to retrieve the same information updates.

Example:



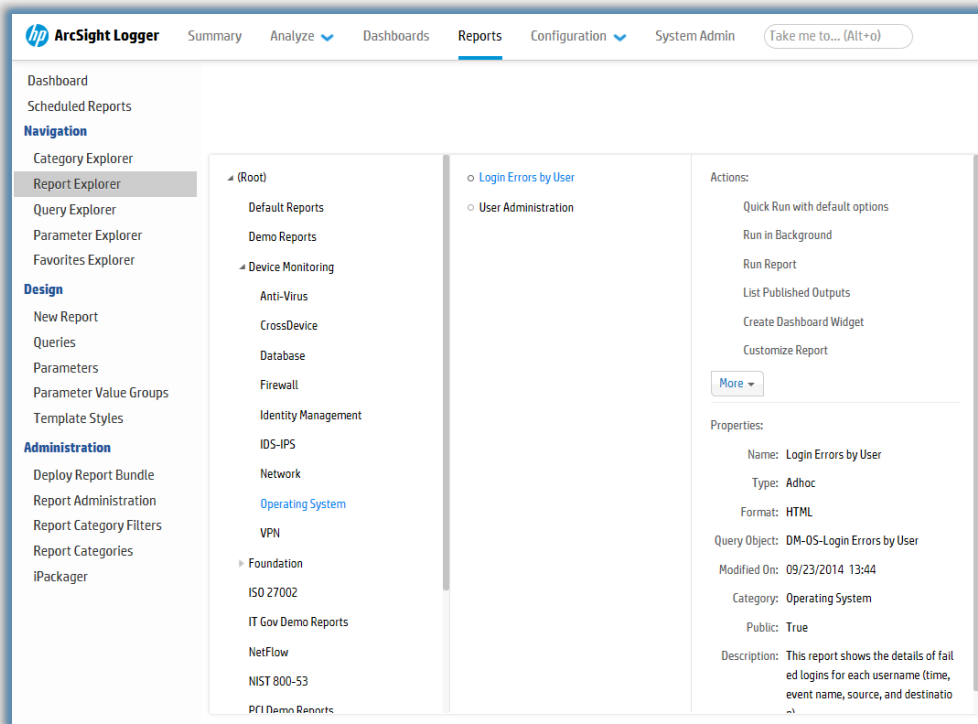
8.6. Running a default report

Choose **Reports** from the Menu

Then under **Navigation** click on **Report Explorer**

In the Reports column choose **Device Monitoring** then **Operating System**

Then choose **Login Errors by User** (Left Example below)



Click on **Quick Run with default options**. Choose **Run Now**

The screenshot shows the HP ArcSight Logger interface. The 'Reports' tab is active, and the 'Login Errors by User' report is selected. The left sidebar contains navigation options like 'Dashboard', 'Scheduled Reports', 'Navigation', 'Design', and 'Administration'. The main area shows report parameters: 'Login Errors by User', 'Start: \$Now - 2h', 'End: []', 'Scan Limit: 100000', and 'Local Only' checked. There are also sections for 'Device Groups', 'Storage Groups', and 'Peers'.

The screenshot shows the 'Login Errors by User' report output. The report title is 'Login Errors by User' and the date is '12/16/2014 12:28 PM'. The table has columns for End Time, Error, Source Zone, Source Address, Source Host Name, Destination Zone, Destination Address, and Destination Host Name. The data shows multiple 'badlogin' errors from various source zones and addresses.

End Time	Error	Source Zone	Source Address	Source Host Name	Destination Zone	Destination Address	Destination Host Name
10/04/2009	badlogin	/All Zones/System Zones/RFC1700	127.0.0.1	localhost	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/Public Address Space/198.20.0.0-222.255.255.255	213.144.137.66	sds1-137-66-init7.net	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/RFC1700	127.0.0.1	localhost	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/Public Address Space/198.20.0.0-222.255.255.255	213.144.137.66	sds1-137-66-init7.net	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/RFC1700	127.0.0.1	localhost	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/Public Address Space/198.20.0.0-222.255.255.255	213.144.137.66	sds1-137-66-init7.net	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System	127.0.0.1	localhost	/All Zones/System Zones/Private	10.0.0.27	

Note that you can save the report in multiple formats such as .csv, .pdf, rtf. You can also email the document or publish it to the portal.



8.7. Creating a report, by customizing default report

Since Logger ships with a variety of useful, pre-built reports for common security scenarios, you can use these not only to run as-is but also as templates for building new reports. If you are just beginning with the Report Designer, a good way to learn fast is to start with an existing report that has some of the features you want in your new report, save the original report under a new name, and then modify it.



Caution

Modifications to reports and other ArcSight-defined content may be overwritten without warning when the content is upgraded. Do not modify ArcSight-defined content directly.

Make modifications to a copy of any ArcSight-defined content as a general practice, and subsequent upgrades will not affect the modifications.

First we want to make a new “**Category**” so that we can have a place to save our reports.

Choose **Reports** from the Menu

Then under “**Navigation**” click on “**Category Explorer**”

Suggestion is to enter your initials such as “**BW Reports**”

Click on “**Save**” (In this case I choose to keep the folder Public)

ADD New Category

Category Name: BW Reports

Category ID: [Empty]

System Generated:

Scope: Public Private Hidden

Buttons: Save, Cancel

Now to customize the report

Rather than create a report from scratch, I am going to:

- Copy the report

- Copy the query

- Change the query

- Change the report to use the new query

- Run the newly modified report.

It is always recommended that you create/copy a standard report into the new category group we just created before making changes. This insures no conflict as ArcSight Supplied updates are provided to you.

We are going to use “**Login Errors by User**” as the basis for our report.

Copy the Report

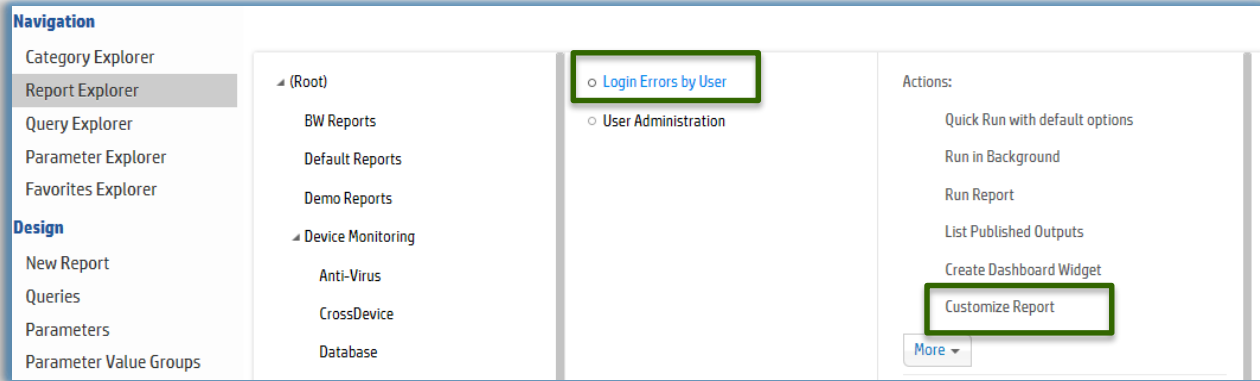
Choose **Reports** from the Menu



Then under “**Navigation**” click on “**Report Explorer**”

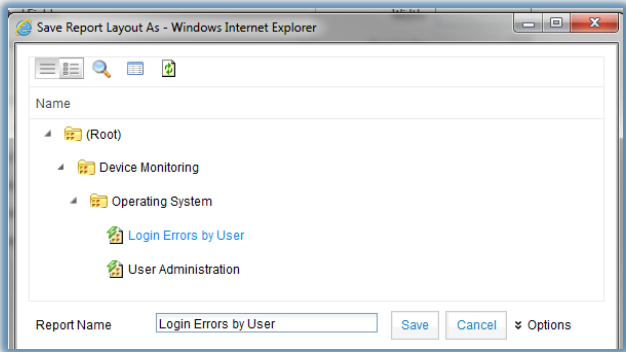
In the Reports column Expand **Device Monitoring** by clicking on the ▲ icon
click “**Operating System**”

Select the report with a Left-Click on “**Login Errors by User**”
When selected it will turn **BLUE**

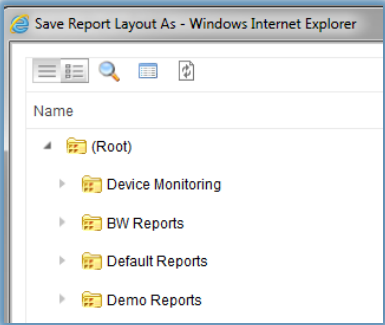


Click on “**Customize Report**”

Click on “**Save As..**” button

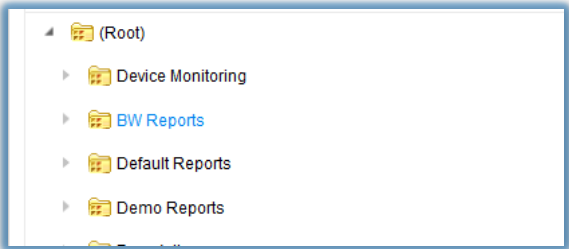


First Step is to refresh the menu by closing the root folder by clicking on the ▲ icon in front of the Root Folder. Then click on it again ▲ to refresh the directory



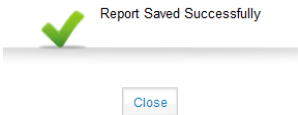
Click on the Folder so it shows that is selected by changing to **BLUE** ▶  **BW Reports**





Report Name Options

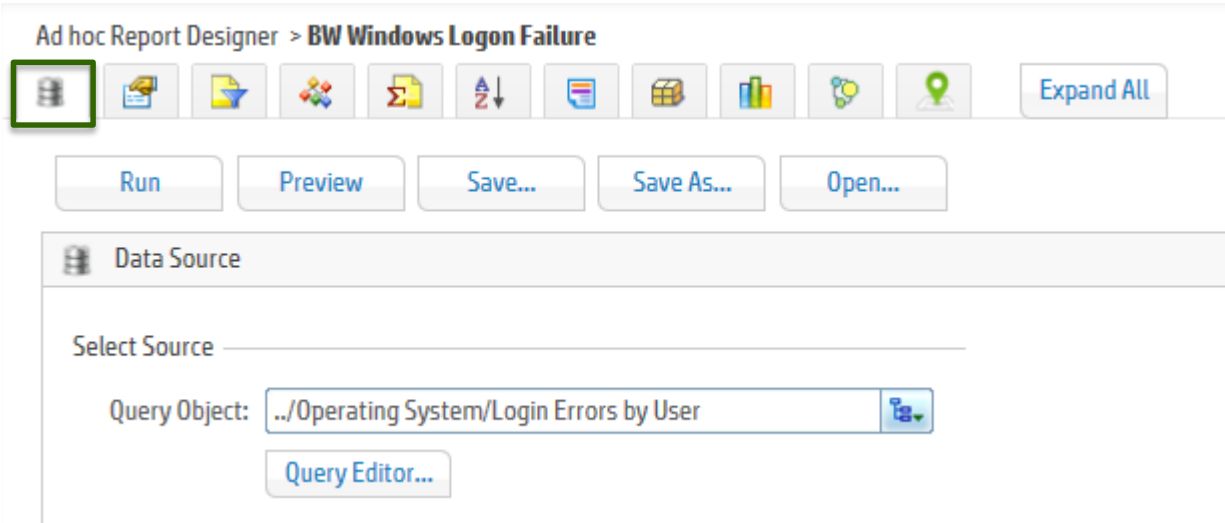
Add your initials in front of the new name you give the report and Click **“Save”**



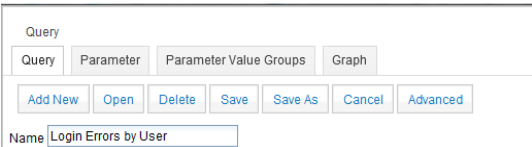
Click **“Close”**

Copy the Query

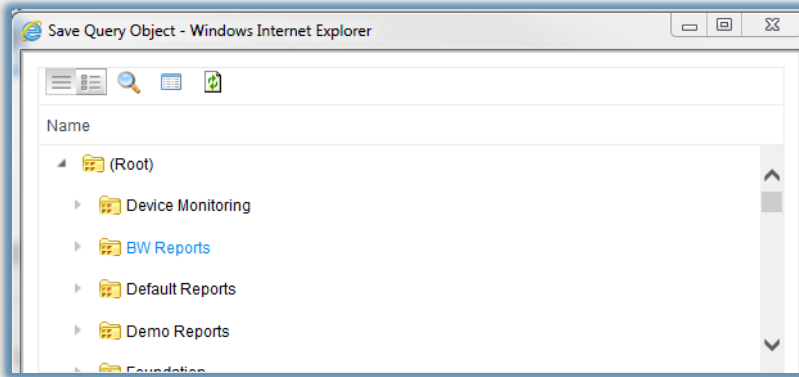
Click on the data source icon



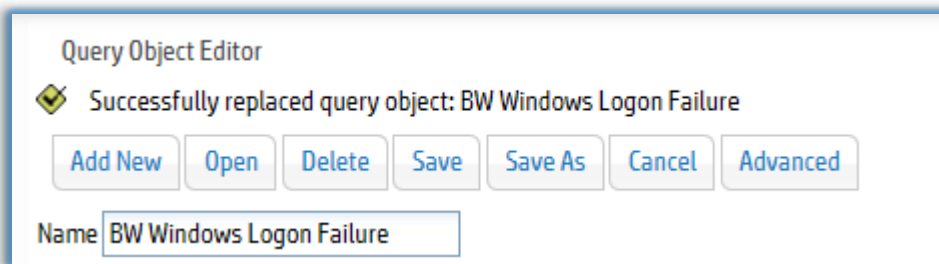
Click on **“Query Editor”**



Now we are going to rename it and save it
Click on the Triangle in front of the root folder and click again to refresh the menu
Click on your folder, in my case “**BW Reports**” to select the folder
Set the Query Object to “**BW Windows Logon Failure**” then click “**Save**”



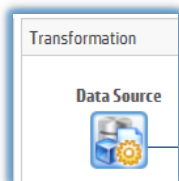
Query Object



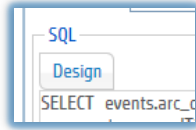
Note the name change.

Change the Query

To edit the query we now click on the new “Data Source” icon



The query appears and we are going to change the where clause.



FIRST you must click on the **“Design”** Icon to expose the editor

```
WHERE events.arc_categoryDeviceGroup = '/Operating System'  
AND events.arc_categoryBehavior = '/Authentication/Verify'  
AND events.arc_categoryOutcome != '/Success'  
AND (  
  events.arc_categorySignificance = '/Informational/Error' OR  
  events.arc_categorySignificance = '/Informational/Warning'
```

To illustrate how we make a change to the SQL we will change the query to only show logon failures and only for device vendor Microsoft.

(In production: we would alter a Parameter to pass the Device Vendor instead of hard coding the device vendor. This was only to expose you to the query editor)

```
SELECT events.arc_destinationUserName "User Name",  
  events.arc_endTime "End Time",  
  events.arc_name "Error",  
  events.arc_sourceZoneURI "Source Zone",  
  events.arc_sourceAddress "Source Address",  
  events.arc_sourceHostName "Source Host Name",  
  events.arc_destinationZoneURI "Destination Zone",  
  events.arc_destinationAddress "Destination Address",  
  events.arc_destinationHostName "Destination Host Name",  
  events.arc_deviceVendor  
FROM events  
WHERE events.arc_categoryDeviceGroup = '/Operating System'  
AND events.arc_categoryBehavior = '/Authentication/Verify'  
AND events.arc_categoryOutcome != '/Failure'  
AND events.arc_deviceVendor = 'Microsoft'  
ORDER BY events.arc_destinationUserName,  
  events.arc_endTime
```

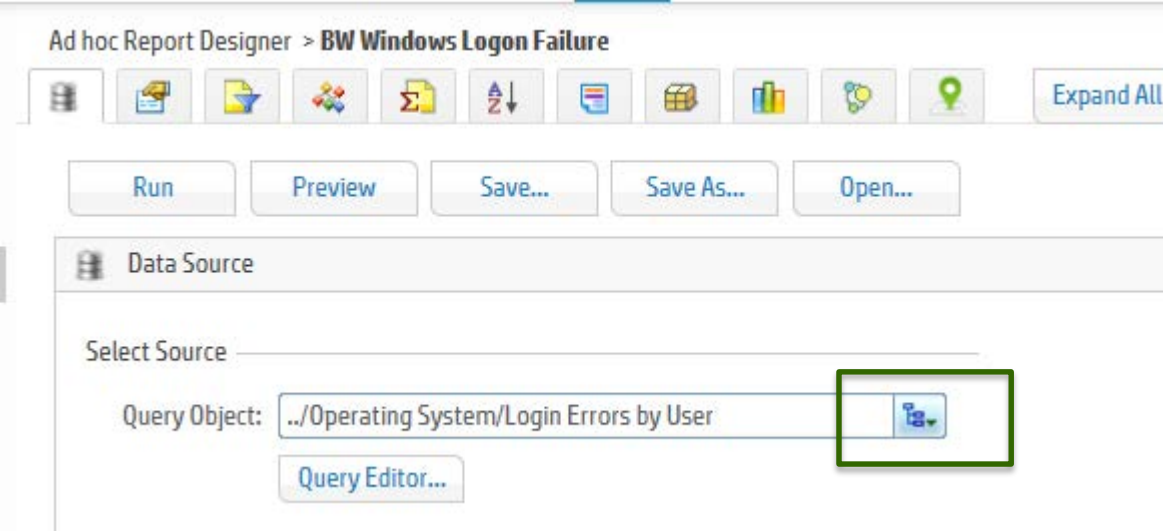
Click **“OK”**

Click **“Save”** or you will lose your changes

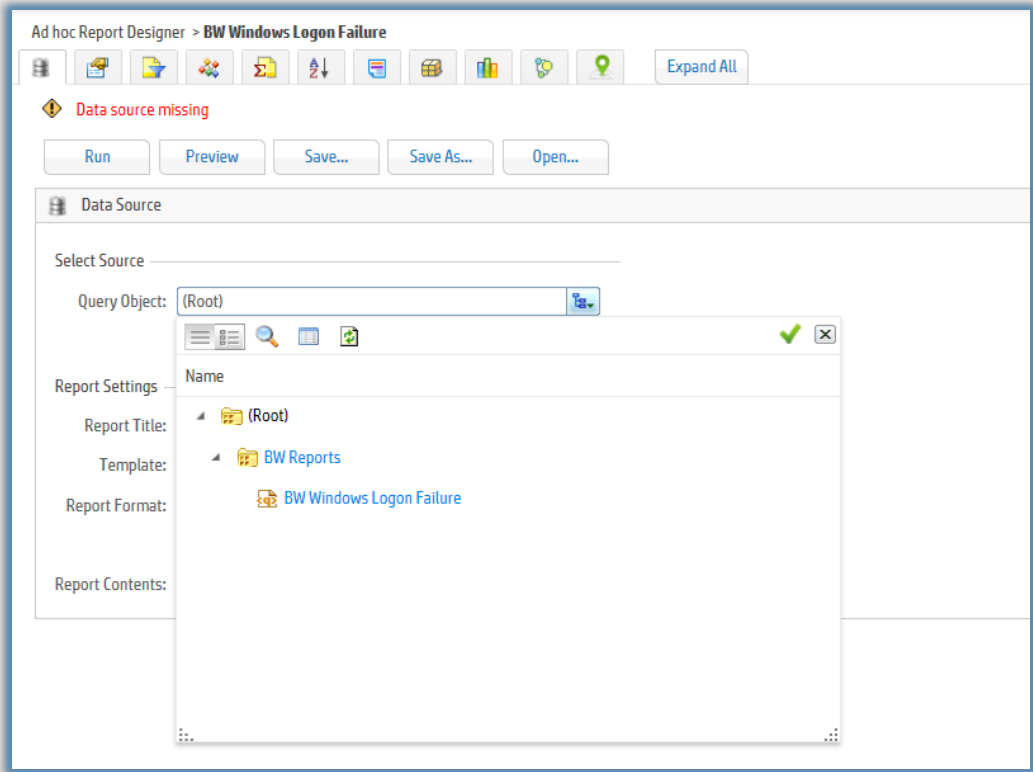
Change the report to use the query

We now need to pair the query with the report by clicking on the **“Data Source”** icon





Change the Query Object by clicking on the “**Root**” folder to close it
Then reopen it to see the BW Reports folder and choose the “**BW Windows Logon Failure**”

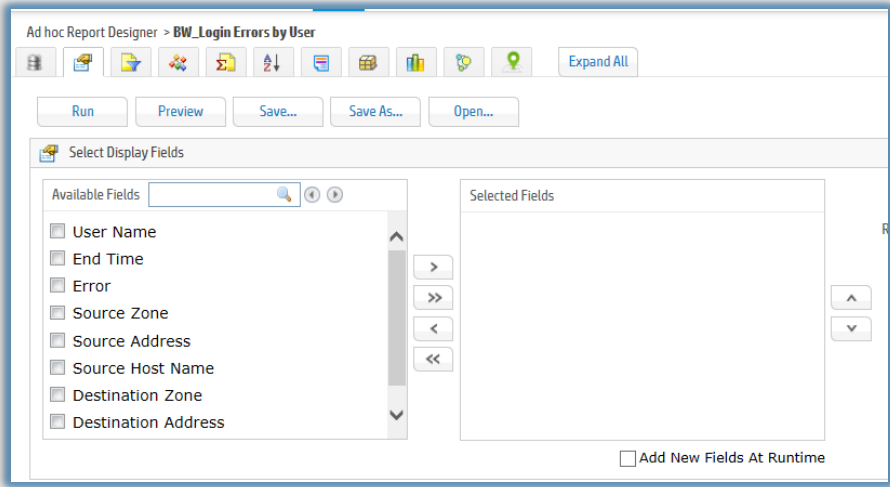



Double Click on “**BW Windows Logon Failure**” if the query object is not already set.

Click “**Save**” and “**Close**”

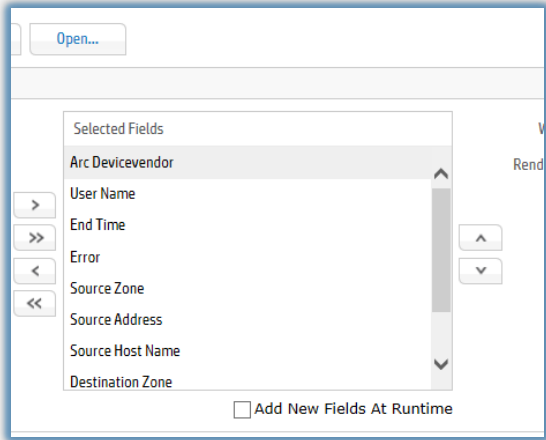


Click on the Fields Editor



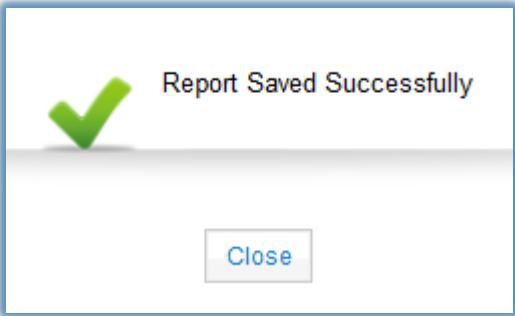
Click on  to select all the fields

Also move the ArcDevicevendor to the top by selecting it and clicking the up arrow till it is at the top.



Click on **Save**





Click "Close"
Click "OK"

Click Run
Click "Run Now"

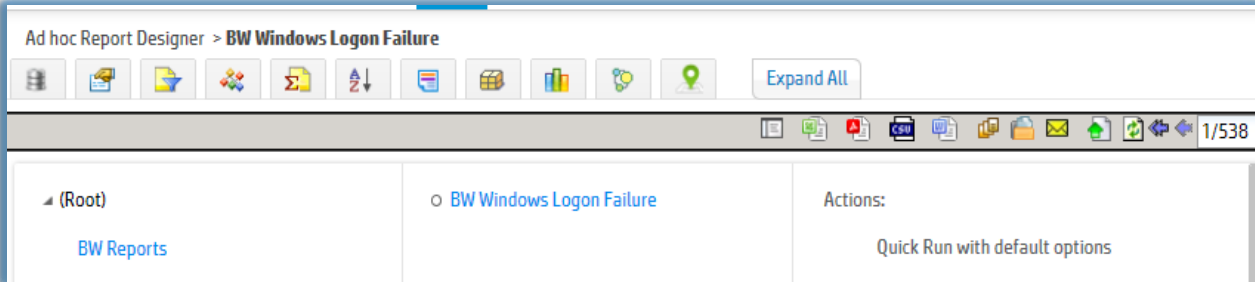
BW_Login Errors by User

12/16/2014 3:02 PM

Start Time:12/16/14 01:02 PM End Time:12/16/14 03:02 PM
Scan Limit:100000

Device Vendor	User Name	End Time	Error	Source Zone	Source Address	Source Host Name
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com

- To run the report:
- Choose "Reports Tab"
 - Choose "Report Explorer"
 - Choose "BW Reports"
 - Choose "BW Windows Logon Failure" from Reports Column
 - Choose "Quick Run with default options"
 - Choose "Run Now"



BW Windows Logon Failure

12/16/2014 8:40 PM

Start Time:12/16/14 06:40 PM End Time:12/16/14 08:40 PM
Scan Limit:100000

Device Vendor	User Name	End Time	Error	Source Zone	Source Address	Source Host Name
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/my2.east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com



9. Pipeline Operators:

Pipeline Operators are critical to refining searches to obtain the information that is sought after. The idea is to add clauses, which are made up of pipeline operators and event attributes, until the search yields the desired results. The order of the pipeline can matter, so think about what it is you want to search for, and how to search for it. Usually, the finished pipeline is a representation of the spoken search process.

Keys – Identifies keys in raw events based on specified delimiters

The keys operator can only be used to determine keys; you cannot pipe those keys into other operators.

Extract – Displays key-value pairs from raw events

Fields – Includes or excludes specified fields

Regex – Selects events that match a specified regular expression

Rename – Renames a CEF or REX extracted field

Replace – Replaces a specified string in one or more specified fields with a new specified string

Rex – Extracts values based on a specified regular expression

Transaction – Group events that have same values in specified fields.

For example, if host and portNum are specified and two events contain “hostA” and “8080”, the events are grouped in a transaction. The transaction IDs created in this search are sorted in ascending order.

Duration - The time in milliseconds of the duration of a transaction, which is the difference between the event time of the last event in the transaction and the first event in the transaction.

Eventcount - Displays the number of events in transactions.

Where – displays events matching criteria specified in “where” expression

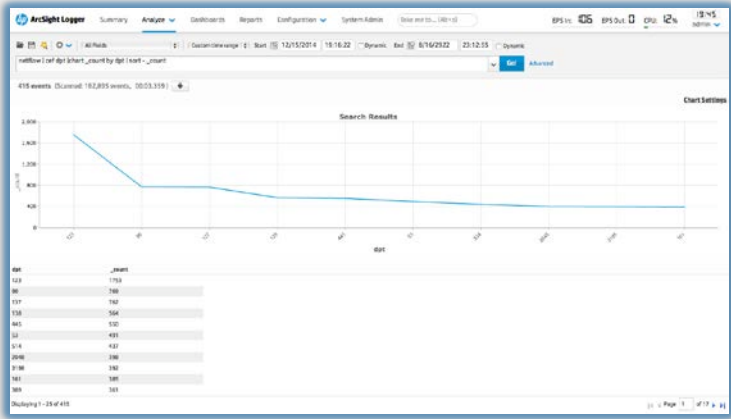
Allows you to use our Field-based operators on Raw events (User-defined Fields extracted from raw events using Pipeline Operators such as rex or extract)



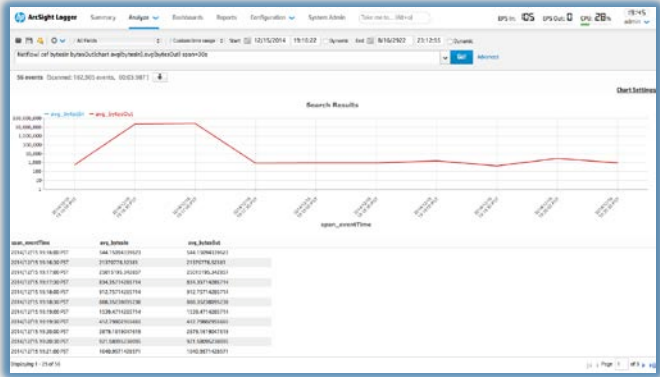
10. Selected Examples:

“What are the counts of destination ports in my Netflow traffic?”
Netflow Chart by count of Events by Destination Port

netflow | cef dpt |chart _count by dpt | sort - _count
Change Chart type to “Line”



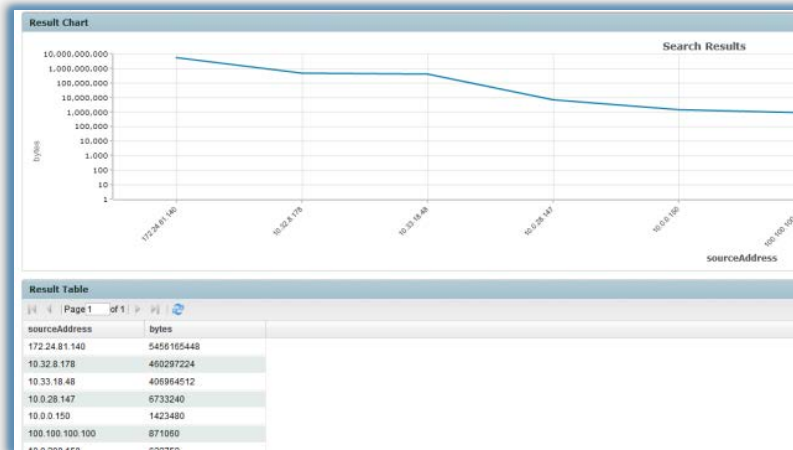
“What are the byte counts, in and out, for Netflow traffic, every 30 seconds?”
Netflow| cef bytesIn bytesOut|chart avg(bytesIn),avg(bytesOut) span=30s



Top Talker:

“What Source Addresses are responsible for the Firewall traffic, and by how much?”

categoryDeviceGroup = "/Firewall" AND categoryBehavior = "/Access" and bytesIn IS NOT NULL | EVAL total_bytes=bytesIn + bytesOut | chart sum(total_bytes) as bytes by sourceAddress | sort - bytes



Here is a search string that will search Blue Coat events, and through using the pipe operator and rex command, will pull out the information after the “q=” in the Google search.

deviceVendor="Blue Coat" | rex "http://www.google.com/search?q\\=(?<term>[^\&&]+)" | top term

If you copy and paste the above expression in to logger, ensure that the double-quotes don't end up as slanty double-quotes in the logger search. This will cause an error in the search. Windows has a way of doing this at times.

Quick Overview of Device Vendors:

| top deviceVendor

Quick Overview of Device Products:



| top deviceProduct

What versions of Connectors are reporting into Logger?

agent:012 | top deviceVersion

How many TippingPoint events per hour?

deviceVendor=TippingPoint | chart sum(baseEventCount) span=1h

What's coming into Logger?

| top name

Failed Logins by User

categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure" AND NOT (destinationUserName IS NULL) | top destinationUserName

Top NetFlow destination ports

destinationPort > 0 AND deviceProduct = "Cisco NetFlow" | top destinationPort

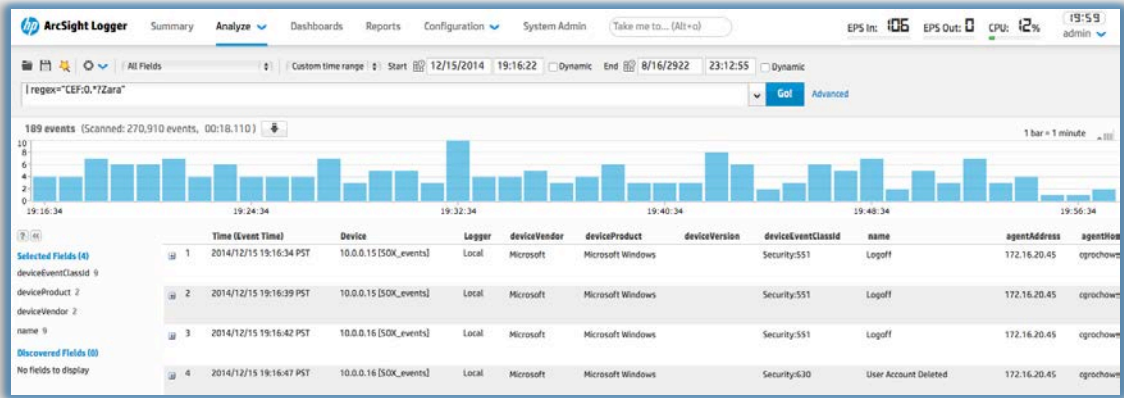
What products have had changes to them recently?

categoryBehavior startswith "/Modify/Configuration" | top deviceProduct

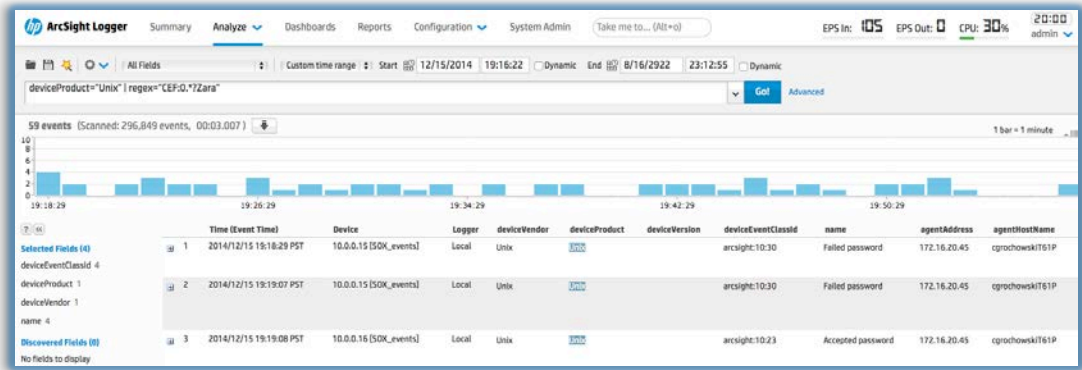


Example of Regex:

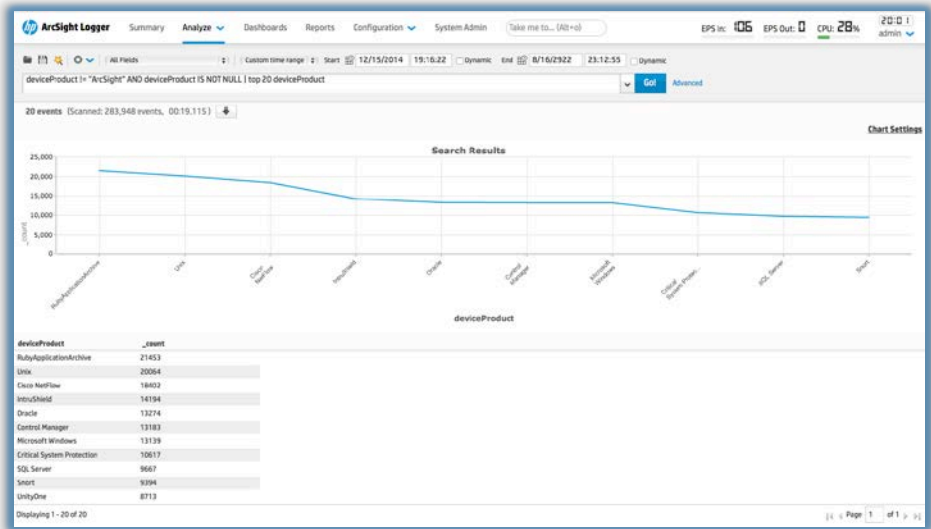
| regex="CEF:0.*?Zara"
14,481 returned



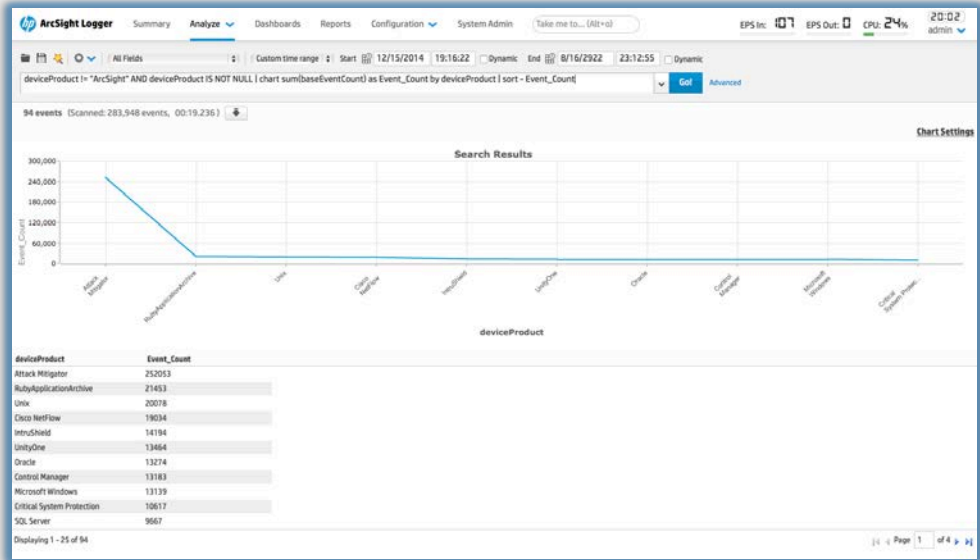
Limit to Unix and username Zara
deviceProduct="Unix" | regex="CEF:0.*?Zara"



Top 20 Products by event count:
deviceProduct != "ArcSight" AND deviceProduct IS NOT NULL | top 20 deviceProduct
(does not account for aggregation, see next query)

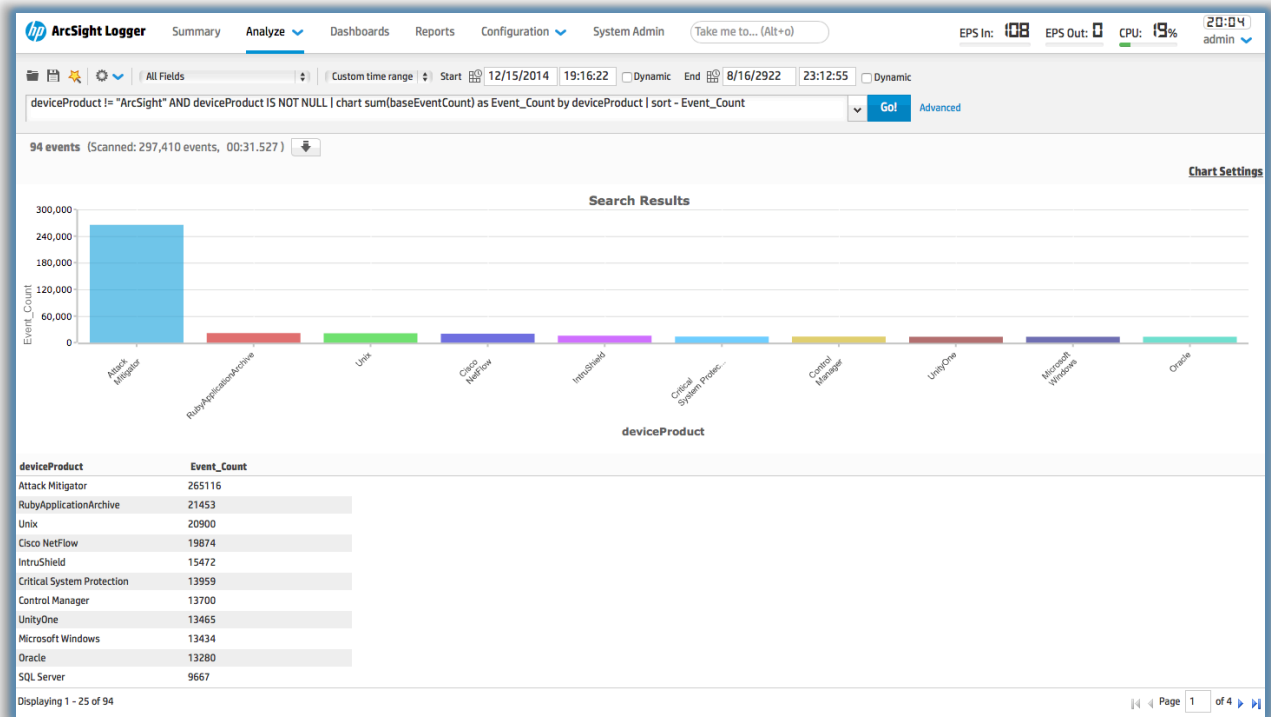


Top 20 products by event count, aggregation used:
deviceProduct != "ArcSight" AND deviceProduct IS NOT NULL | chart sum(baseEventCount) as Event_Count by deviceProduct | sort - Event_Count



How many events by each source from highest to lowest:

deviceProduct != "ArcSight" AND deviceProduct IS NOT NULL | chart sum(baseEventCount) as Event_Count by deviceProduct | sort - Event_Count



Blue Coat Bytes In and Bytes Out

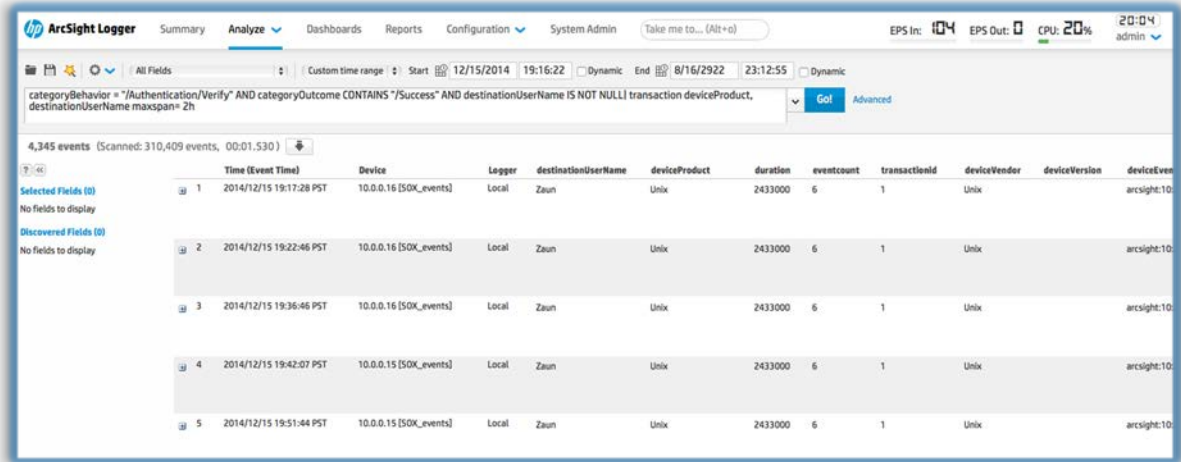
deviceVendor="Blue Coat" and destinationHostName is not null AND NOT destinationHostName CONTAINS "windowsupdate" | chart sum(bytesIn) as TTLBytesIn, sum(bytesOut) by sourceAddress | sort - TTLBytesIn

deviceVendor="Blue Coat" and destinationHostName is not null AND NOT destinationHostName CONTAINS "windowsupdate" | chart sum(bytesIn) as TTLBytesIn, sum(bytesOut) by sourceAddress | sort - TTLBytesIn



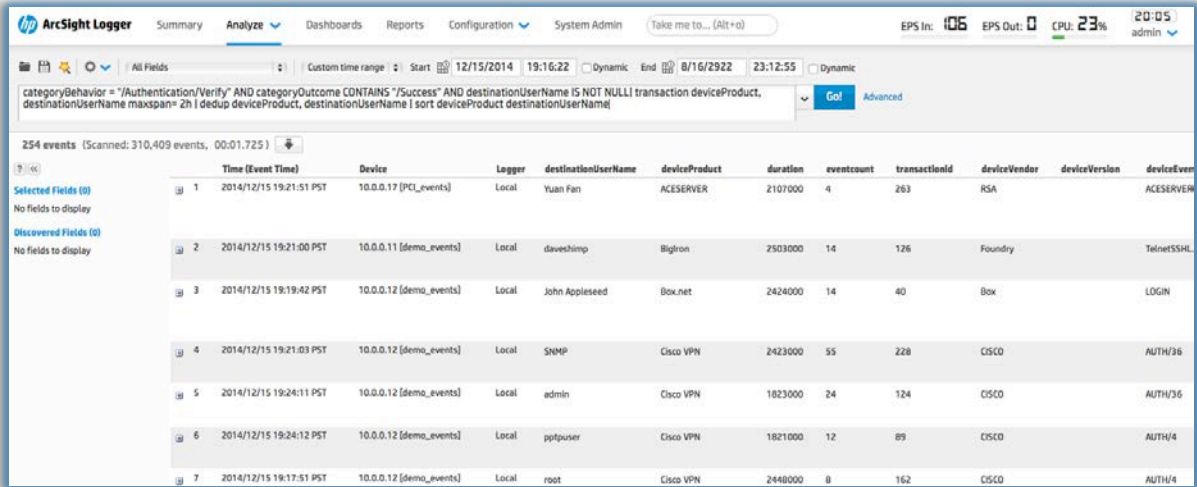
Transaction

categoryBehavior = "/Authentication/Verify" AND categoryOutcome CONTAINS "/Success" AND destinationUserName IS NOT NULL| transaction deviceProduct, destinationUserName maxspan= 2h



Transaction and De Duplication

categoryBehavior = "/Authentication/Verify" AND categoryOutcome CONTAINS "/Success" AND destinationUserName IS NOT NULL| transaction deviceProduct, destinationUserName maxspan= 2h | dedup deviceProduct, destinationUserName | sort deviceProduct destinationUserName



11. Reporting Example

If you have two loggers peered, how can you report on the Average EPS per day per Logger

Here is the query, and with Logger 6.0 we wrote this report. Each Line in the chart is a Logger in the peer group. And those lines in the chart are a little bit interactive, where you can scroll and Logger will change and show the values.

The query

```
SELECT
DATE(events.arc_deviceReceiptTime) as "Date",
events.arc_deviceAddress as "Logger",
AVG(events.arc_deviceCustomNumber1) as "Average EPS"
FROM events
WHERE
events.arc_deviceEventClassId = "eps:100" AND
events.arc_deviceAddress IS NOT NULL
GROUP BY
events.arc_deviceAddress,
DATE(events.arc_deviceReceiptTime)
ORDER BY
DATE(events.arc_deviceReceiptTime)
```

