Methodology for McAfee Enterprise Security Manager (ESM) Employment

Version 1.0
Date: 9-31-2016
POC: @Wired_Pulse

Date	Version	Changelog	Pages	By
4-13-2016	1	Document creation	All	@Wired_Pulse
9-31-2016	1.1	Moved ESM PS script from document to my github	93	@Wired_Pulse

Table of Contents

Introduction

McAfee Enterprise Security Manager (ESM) is a security information and event management (SIEM) system that delivers the performance, actionable intelligence, and near real-time situational awareness required to identify, understand, and respond to stealthy threats. ESM can receive data via an agent or through agentless methods.

From a defensive perspective the agentless method allows the team to be less intrusive yet still get the oversight and data they require in order to support the supported organization. ESM can ingest logs from a wide array of systems and programs to include Windows event logs, Snort, Bro, and HBSS. A full list of data sources can be found at https://kc.mcafee.com/corporate/index?page=content&id=PD25060.

Once data is ingested, custom correlation views and dashboards can be made to provide a holistic view of events taken place in the organization.

This guide was developed using ESM 9.5. As such, using any other version may show that some of the TTPs mentioned here are not applicable.

Methodology

1) Retrieve logs
2) Set Policies to help parse logs based on certain criteria
3) Create Dashboards to show data from a holistic view

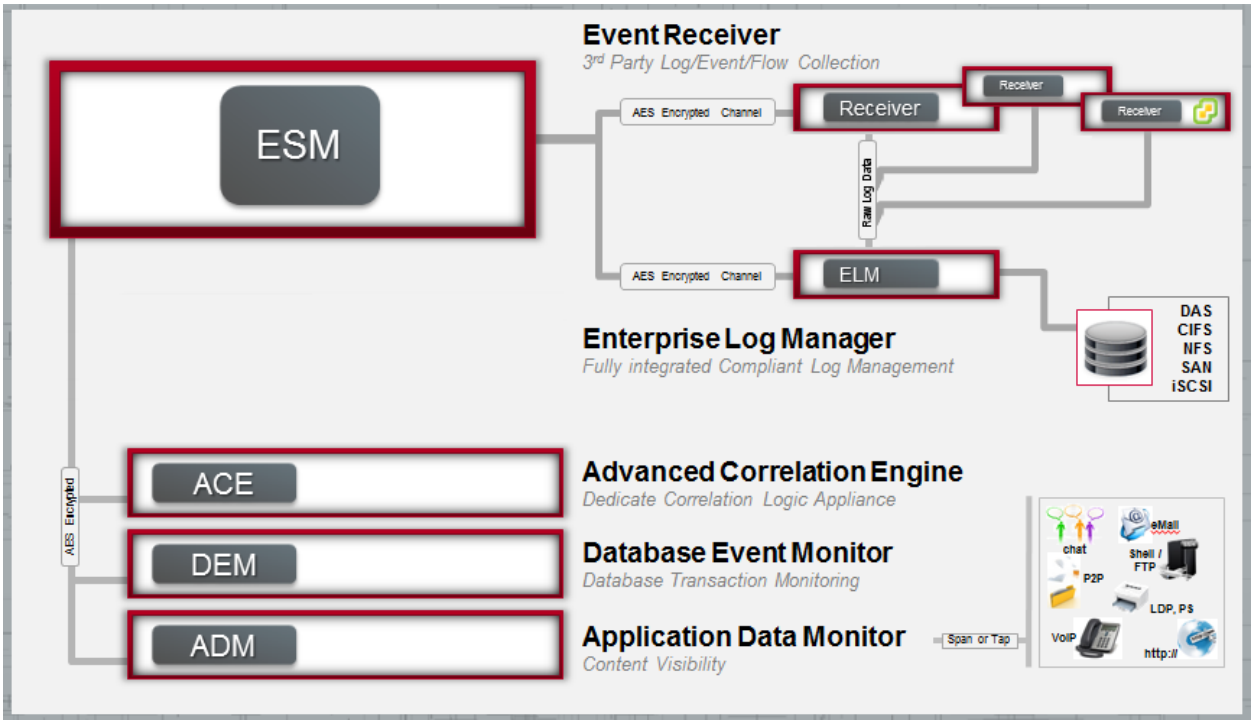
Server Download

At the moment, ESM is supported in Inc2 through PEO C3T so depending on the mission, it may be available to you through this avenue. In all other cases, McAfee has full-fledged instances of ESM and Advance Correlation Engine (ACE) available to you in approximately 4-5 trial blocks. Those VMs can be found at http://www.mcafee.com/apps/downloads/free-evaluations/default.aspx?pc=productcategory&pg=1&pid=&eid=&sz=25&srt=description&sd=ASC&segment=false&region=us.

Components and Requirements

Server Components

ESM consists of three components: Receiver, Enterprise Security Manager (server), and Enterprise Log Manager (ELM). While these components can be distributed from McAfee in an appliance form, the defensive elements can utilize ESM as 'combo VM' – meaning that all three ESM components are on a single VM (i.e., not distributed).



Purposes

Receiver:

- Parses received packets that contain syslog data, Windows logs, and netflows from devices ('pushed' to Receiver)
- Pulls events from myriad of devices but defensive elements could specifically utilize it for Windows event log collection
- Parses, aggregates, normalizes, correlates received events
  - Aggregation: consolidate virtually identical syslogs entries within a time period into a single event (with count). Helps to reduce 'noise'.
  - Normalization: classify each event into an Event Type and a Sub-Type, using 'normalized' names.
  - Correlation: generate new events based on received events that matches a correlation rule loaded into the Receiver (e.g., Possible Brute Force Attack event).

Enterprise Security Manager (ESM) Server:

- Pulls events from Receiver
- Database for storing the events, logs, netflows. Parsed data written to disk.
- Secure Web Server provides user interface (UI)

Enterprise Log Manager (ELM):

- Stores raw events & logs to disk received from data sources.
- Data is signed & compressed when written to disk.

Advanced Correlation Engine (ACE):

- Receives notifications if specific users, groups, applications, servers, or subnets are threatened.
- Get alerts if threats target your priority users, assets, applications, and activities.
- Simplify event correlation and startup. No rule updates or signature tuning required.
- Uses audit trails and historical replays to support forensics, compliance, and rule tuning.

VM Requirements

It is recommended that the ESM VM be equipped with the following:

- At least 4 cores or vCPUs but recommend 6 cores or vCPUs
- At least 500 GB disk space but recommend at 1 TB
- 16 GB RAM

Web UI requirements

Access to the ESM web UI requires the following:

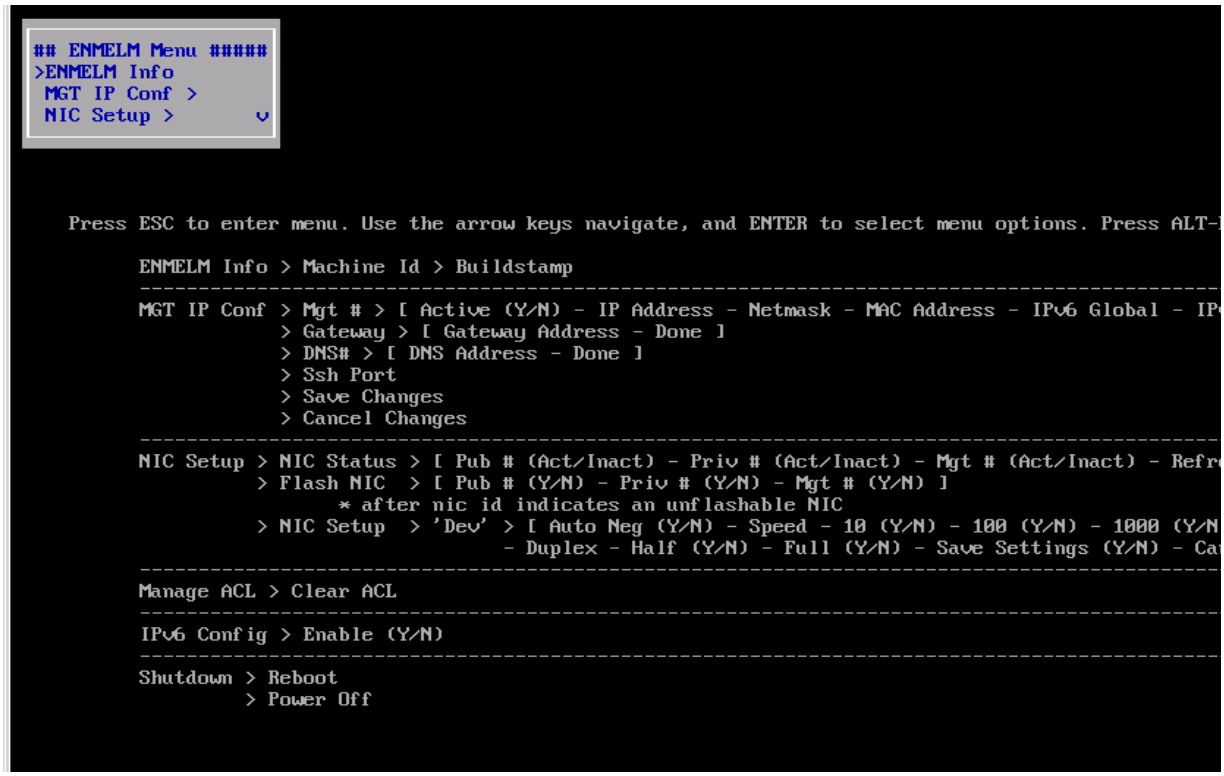
- A browser with Flash player version 11.2 or later.
- Browser pop-up blocker disabled for the ESM's IP address

ESM has a secure web interface – requiring SSL/TLS. Therefore you must always use "https" for web access into ESM.

Server Setup

Configuration

1) Obtain the VM, load it in your hypervisor, and power it on
2) Upon successful booting, you will be presented with the following window



3) Click inside the window and press ESC to access the menu in the grey box.
4) Use the down arrow key to position cursor arrow next to “MGT IP Conf” selection and then hit Enter key.
5) If necessary, move cursor arrow next to “Mgt1” and then hit Enter key.
6) If necessary, move cursor arrow next to “IP Address” and then hit Enter key.
7) Type in the IP that you wish to give the system. Be sure that the entered IP address is correct and then hit Enter key.
8) Move cursor arrow next to “Netmask” and hit Enter key.
9) Type in the netmask that corresponds with the above IP. Be sure that the entered Netmask is correct and then hit Enter key.
10) Move cursor down to “Done” and hit Enter key.
11) Move cursor down to “Gateway” and hit Enter key twice.
12) Type in the gateway for the network. Be sure that the entered address is correct and then hit Enter key.
13) Move cursor down to “Done” and hit Enter key.
14) Move cursor down to “DNS1” and hit Enter key twice.
15) Type in the DNS IP. Be sure that the entered address is correct and then hit Enter key.
16) Mover cursor to “Save Changes” and hit Enter key.

Note: It may take a few minutes after configuring the network settings before you are able to access the VM via the web interface.

17) Open a browser and navigate to the IP of the ESM (ex: https:\\IP_Address_of_ESM)
18) Log in with any credentials that you were provided. If you were not provided any, try the McAfee default credentials.

    User: NGCP
    Pass: security.4u

19) If this is the first time that ESM has been logged into, you will be prompted to do the following:
    - Read and accept the EULA
    - Change the password
    - Decide whether to use FIPS mode or not (it is recommended not to)
    - Set the time zone (recommended to use UTC)
    - Input a NTP server (optional)
    - Input your customer ID (optional)
20) Once complete, click Finish. The system may inform you that it is restarting. If not, you will be able log in again. After successful login, you will be presented with the ESM main screen consisting of a dashboard.

Key Device

For ESM to communicate with a device, it must encrypt all communications using the communications key that is created when the device is keyed. In order to achieve that, do the following:

1) Open the Receiver Properties and select Key Management
2) Select “Key Device”
3) Enter a password of your choice
4) Click Next
5) Once the successful message is displayed, click finish
6) Select OK

Additional User Creation

During the initial installation of McAfee ESM, you logged in and performed initial configuration with the "NGCP" user. It's best to create additional administrative accounts to use for daily operations. This provides better accountability for individual users, and also ensures access to the ESM console is available, even if the NGCP password is lost or forgotten.

To create admin users, create administrative user accounts:

- Log into ESM as NGCP open the ESM System Properties, and select the Users and Groups tab.
- Enter the NGCP password when prompted.
- Define a new user (if necessary) and select the "Administrator Rights" checkbox.

Configure Local Network

ESM uses the Local Network setting to identify IP addresses that are considered to be “inside” your enterprise network. This variable is used in a wide range of correlation rules and other ESM components

to differentiate between inbound and outbound traffic. It's important to configure this setting properly in order for rules and other SIEM features to operate properly.

To configure the Local Network:

1) Open Asset Manager.
2) Select the Network Discovery tab and click Local Network.
3) Enter the IP range that defines your internal network. The local Network is defined as a comma-separated list of IP addresses and/or IP ranges.
4) Click OK to save.

ESM Interface

Interface Orientation

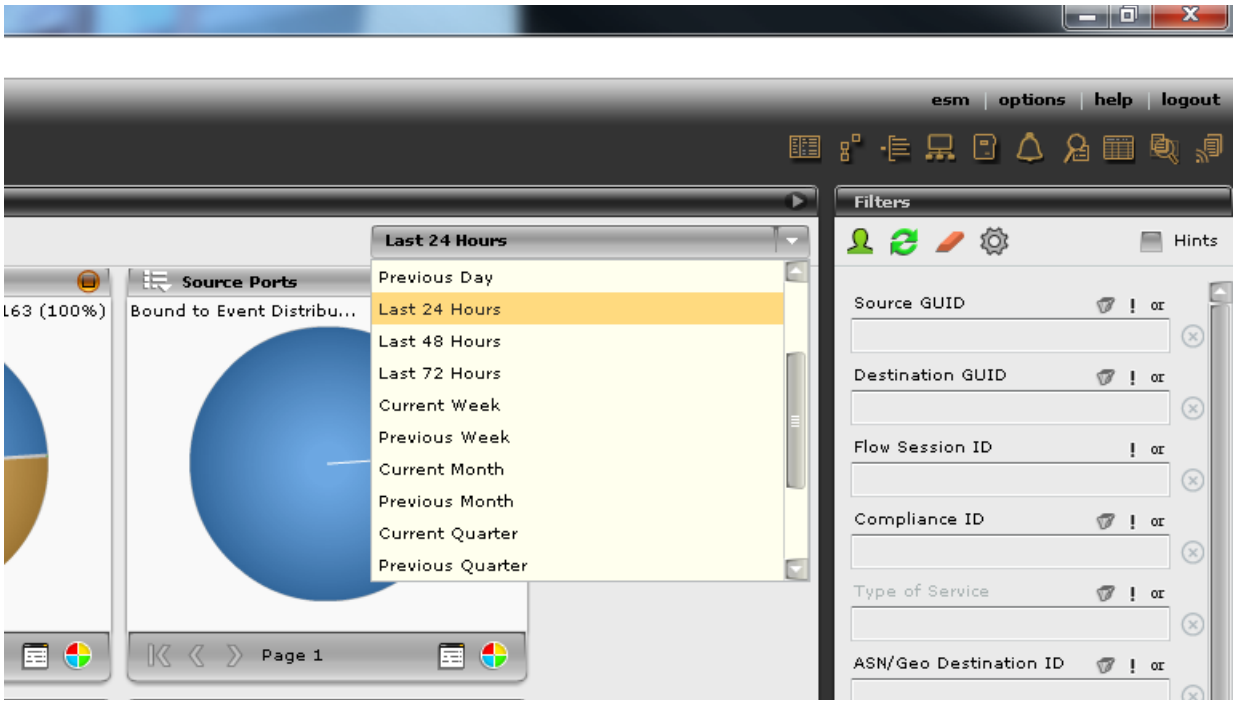
Defenders have the ability to shape the interface into views that contain numerous different displays of information, and creating these and switching among them are incredibly simple. The ESM interface is composed of several distinct panes:

- Event Summary: Displays major malicious events detected
- Source IPs: Displays source IP addresses noted in events
- Total Events: Displays a simple metric for keeping up with overall event counts in the environment
- Event Distribution: Charts event counts as a graph over time
- Destination Geolocation: Displays the location of events in a specified period

This is discussed more in the dashboard section of this document.

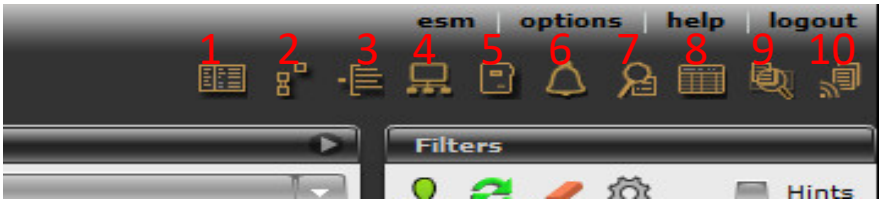
In the uppermost right corner of the above window is a drop-down menu for specifying the time range viewed, with built-in ranges from the last minute to several years. Custom ranges can be set easily as well.

A depiction of the timeframe setting is displayed below.



Quick Launch Menu

In the upper-right corner of the ESM interface, there are “Quick Launch” icons that direct users to important product features.



The quick launch provides access to the following functions and capabilities. The numbers in the picture correspond with the numbers below.

1) System Properties. This contains information about the system, its hardware platform, application and OS licenses and other basic details.
2) Policy Editor. The platform’s rule engine operates in a variety of categories, ranging from intrusion prevention system (IPS) signatures to firewall rules, database monitoring, and others.

3) Correlation. This icon accesses the correlation engine, which combines policy rules and custom parameters to create complex filtering and alerting definitions that only trigger alerts when several conditions are met, such as IPS rules and specific source addresses appearing together.
4) Asset Manager. The Asset Manager polls devices discovered on the network for their configuration details. It can group discovered assets into zones for risk classification and identification, and is useful in configuring network discovery tasks.
5) Reports. You can set ESM to generate reports on the fly or according to a schedule. The reports can be custom or standard reports provided through ESM.
6) Alarms. These can send a variety of alerts, which can be aggregated into a simple view, to analysts. For example, an analyst could have an alarm triggered by a specific threshold of traffic, or certain types of rules that were triggered, and ESM could send an e-mail notifying the team.
7) Watchlists. These can monitor for specific objects or identified systems, users, traffic, protocols, ports, addresses and more. When the targeted object is spotted, a rule will then notify an assigned analyst.
8) Case Management. In this feature, you can create and track event "cases." This is a simple incident tracking system that functions in a manner similar to basic ticketing applications.
9) Enterprise Log Manager (ELM) Search. This feature queries specific log events if ESM is connected to McAfee's Enterprise Log Manager.
10) Cyber Threat Indicators. This feature lists the received IOCs and the number of times it hit against data in ESM.

Filter Menu

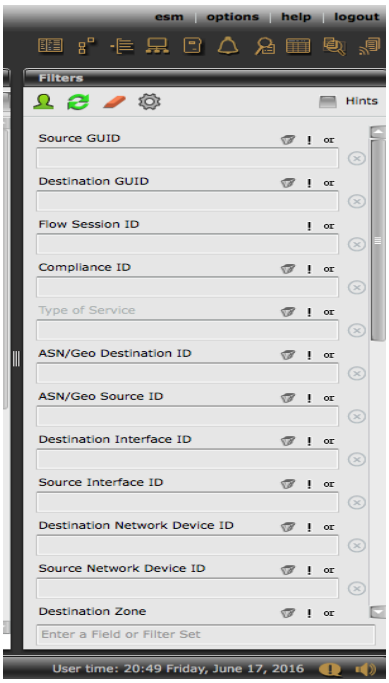
The filter menu allows for one to quickly search for the data they desire. This can be completed by a myriad to factors. By default, some of the most common one will be shown but you can search based upon other criteria as well. Begin typing in the field at the bottom of the filter pane. Custom filters can be made as well by clicking the gear icon and then selecting "Manage Filters". From there, folders can be created along with filters.

Data Filtering

There are several concepts that you will use repeatedly when investigating incidents. By learning to take advantage of these up front, you will streamline your interactions with the console. Below is a video that highlights the basics of working with views and dashboards.

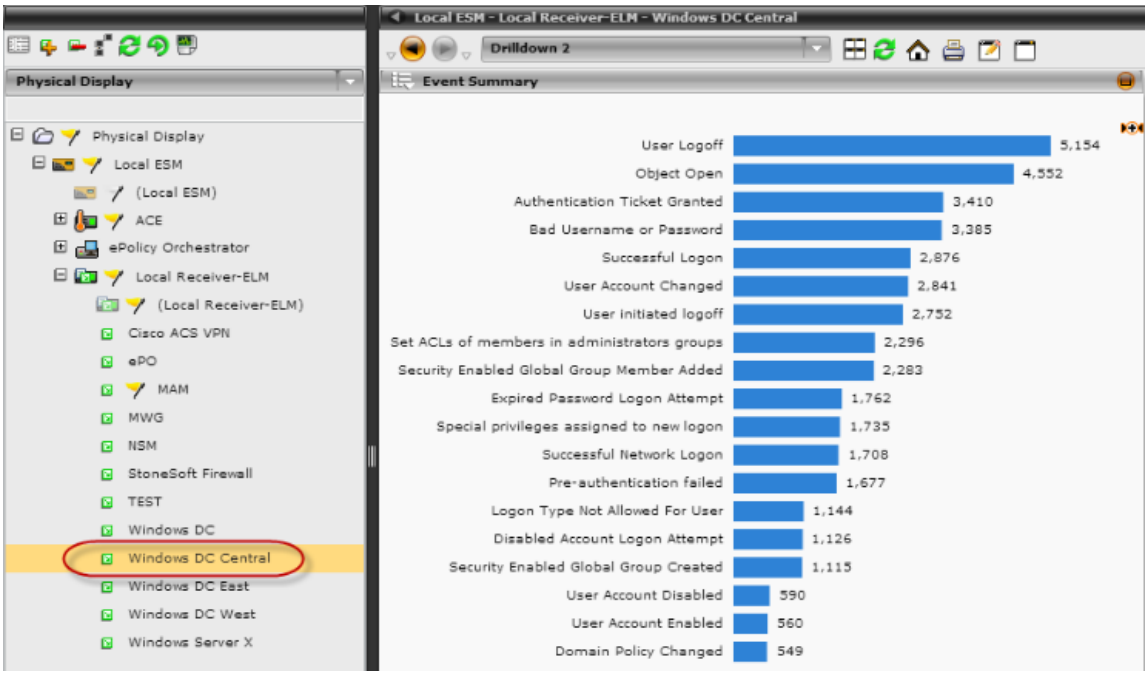
Filter Menu

The filter menu allows for one to quickly search for the data they desire. This can be completed by a myriad to factors. By default, some of the most common one will be shown but you can search based upon other criteria as well. Begin typing in the field at the bottom of the filter pane. Custom filters can be made as well by clicking the gear icon and then selecting "Manage Filters". From there, folders can be created along with filters.



Filter by data source

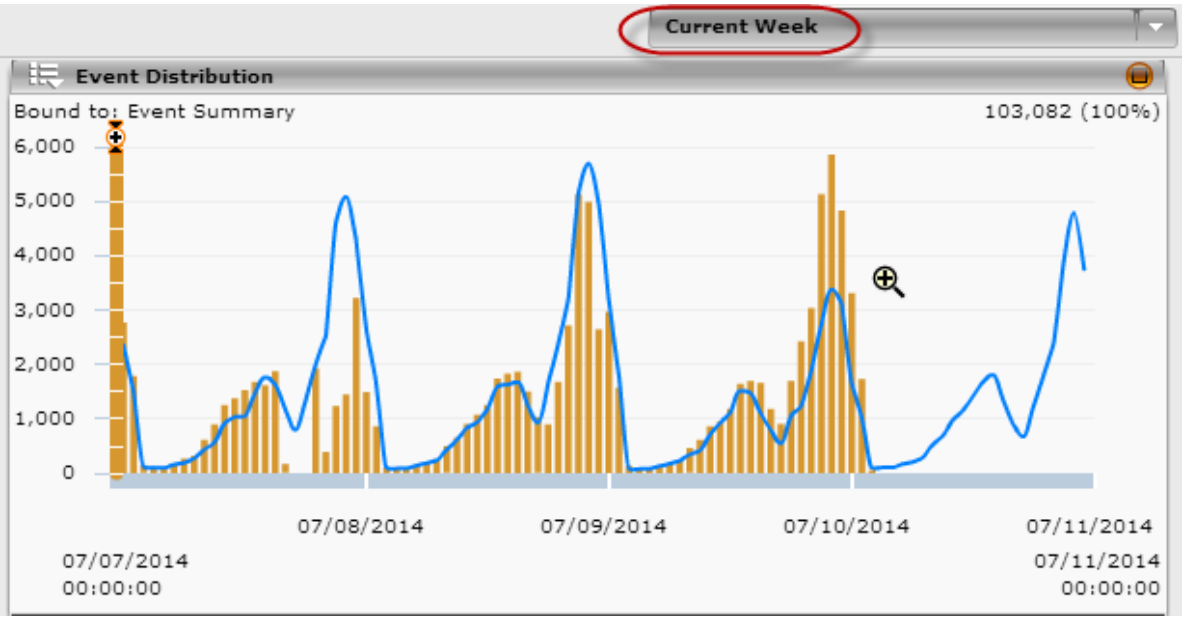
Most views and dashboards, by default, display a wide range of data. There are times when you might like to have a view display data for a specific data source. By selecting the data source in the system tree in the left panel of the SIEM console, you will automatically filter to show only events from that source.



You can shift-click and control-click to select multiple data sources. You can also leverage the Display popup at the top of this panel to change how your data sources are shown. For example, changing from Physical Display to Device Type Display groups all your data sources by type, allowing you easily to group similar data sources together.

Filter by time

Other times you will want to see events for a particular time range. Perhaps you need to run a report for a particular week, or are investigating an incident that happened on a known day in the past. The time filter in the top-right corner of the SIEM console gives you a great deal of flexibility in selecting specific time frames



It's helpful to understand conventions used for naming time filters.

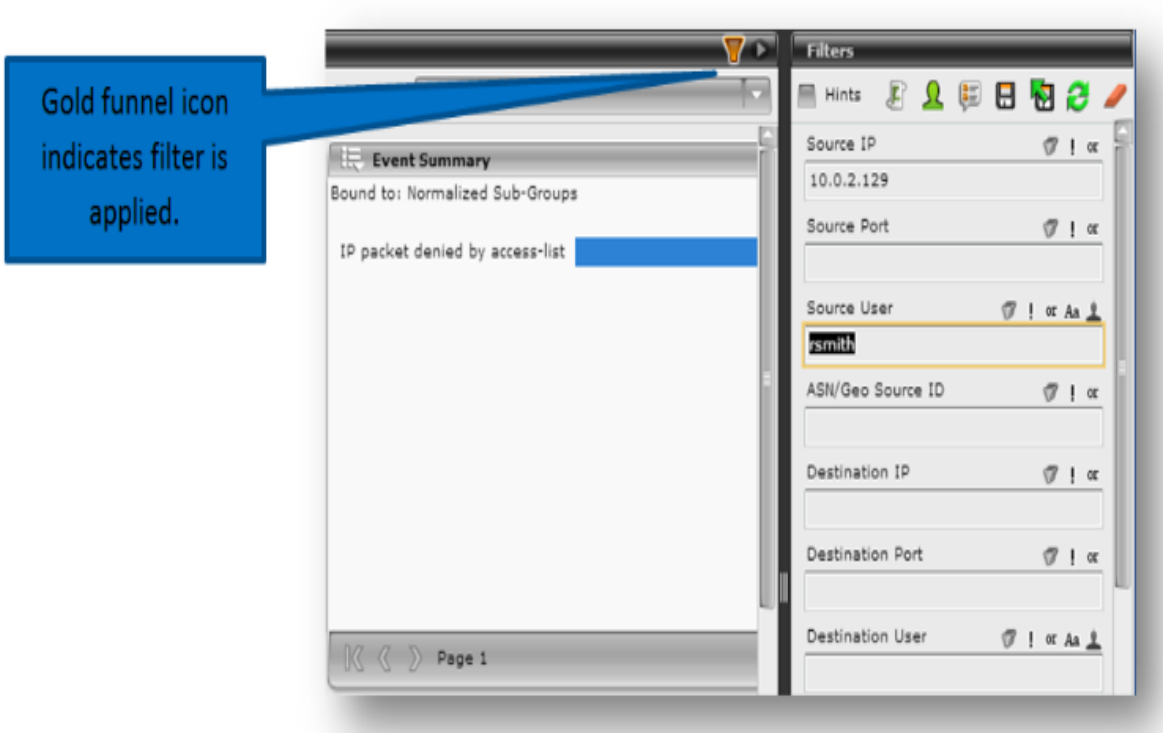
- "Current": the time period we are in the middle of right now. For example, if today is June 10th, and you set a filter to show "Current Month", you will see data from June 1 – June 31. Since events for June 11-31 have not happened yet, you will only see 10 days' worth of events with this filter, in this example.
- "Previous": the previous time period. For example, if today is June 10th and you set a filter to show "Previous Month", you will see data from May 1 – May 31.
- "Last": the last 24, 48, or 72 hours. For example if the time is 11:00am EST and you set the filter to show "Last 24 hours", you will see data starting from 11:00am EST the previous day to 11:00am EST the current day.

Note: You can always select "Custom Time" to set very granular time filters, if necessary.

Filter by other fields

The right-side panel in the ESM console is called the filter panel. This panel allows you to create ad-hoc queries very simply, by filling in the proper fields. To apply a filter, simply enter the desired criteria into the filter panel, and hit Enter, or refresh your view. When the filter is applied, a gold funnel icon will

appear at the top of the view panel as an indicator.

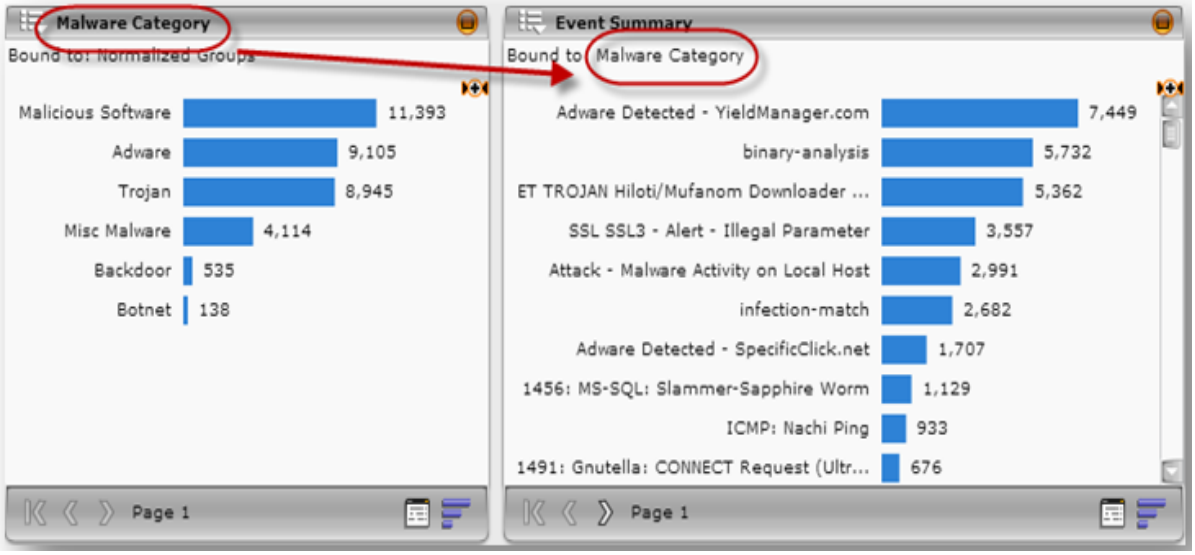


By default, ESM displays a limited set of filter options. You can control the filter options displayed via the row of icons at the top of the filter panel:

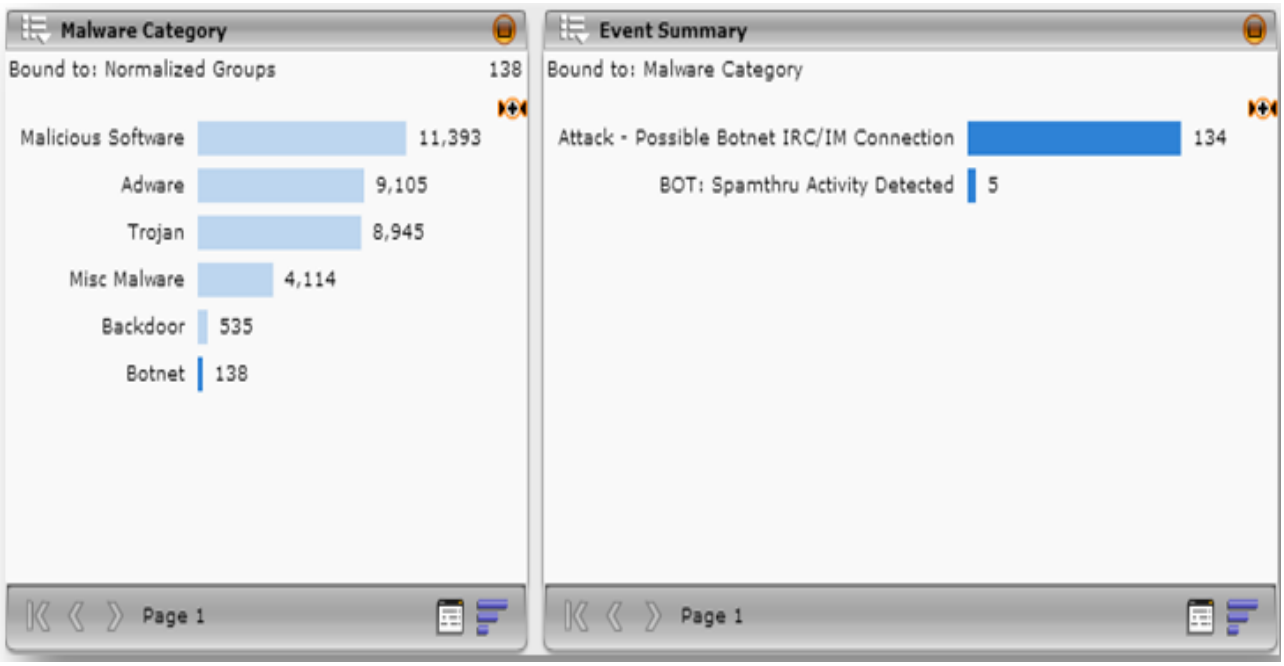
When multiple filters are defined in the filters panel, they are all combined by default with "AND" logic. Other logic options are available via the icons above each field. Each field provides options for entering multiple filter criteria; enable Hints via the checkbox at the top of the screen for full description of the options for each filter field.

Filter by view binding

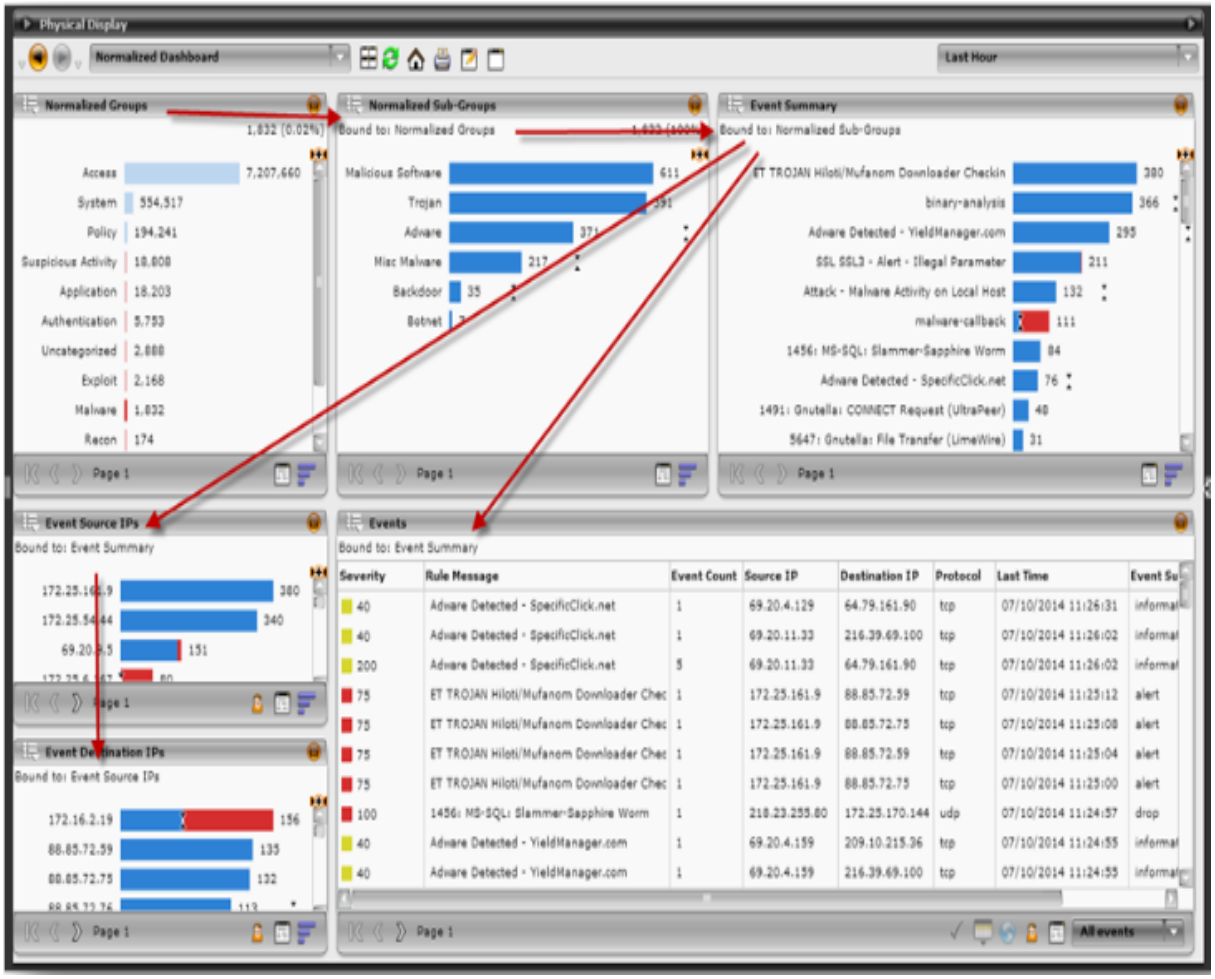
Binding is a powerful concept that allows panes in a view to act as filters on each other, allowing you to quickly drill into data elements that are most interesting to you. When a view pane is bound to a pane above it, making a selection in the parent pane acts as a filter on the child pane. Below is an example.



In the example above, we see thousands of malware related events. The panel on the left shows the malware event category, and the right-hand panel provides details. The right panel (Event Summary) is bound to the left panel (Malware Category). By making a selection in the Malware Category pane, the Event Summary pane is automatically filtered to show only the events with the selected Malware Category (in this case, 138 Botnet events):



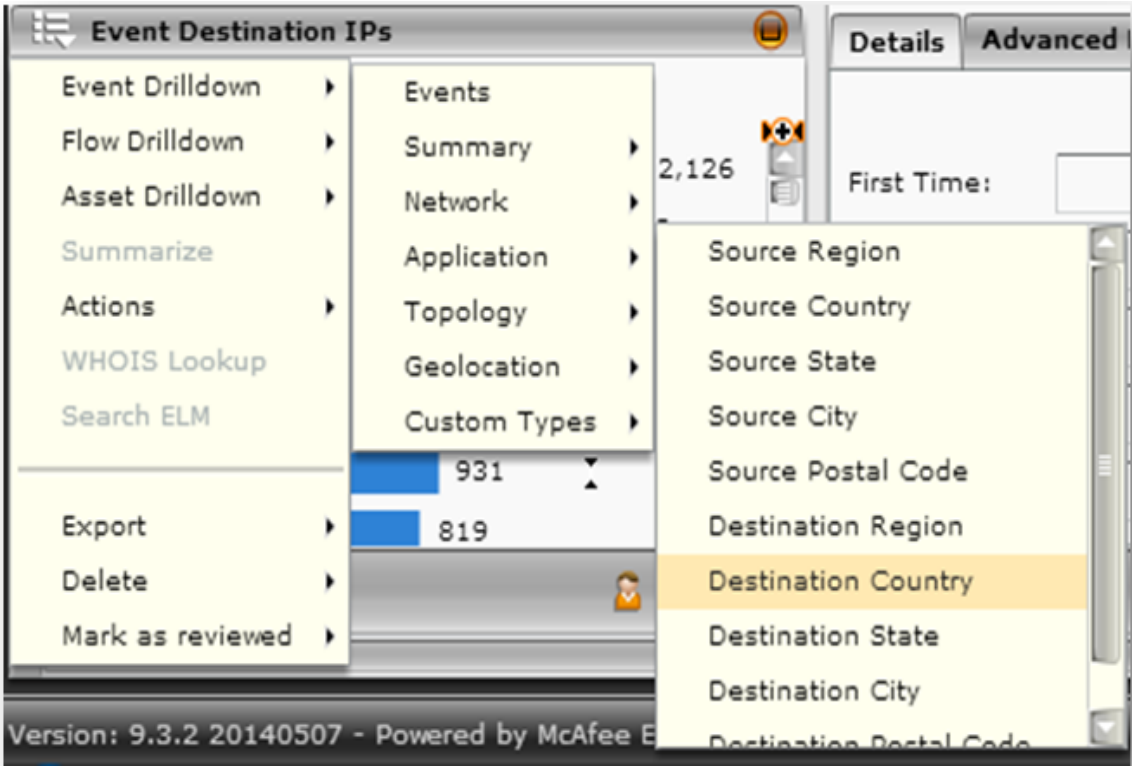
Panels in a view may be configured with cascading bindings, such that a selection at a high-level panel cascades to all the panels in a view. The example below shows how a single selection in the Normalized Groups pane (top left corner) becomes a filter that flows to the rest of the view.



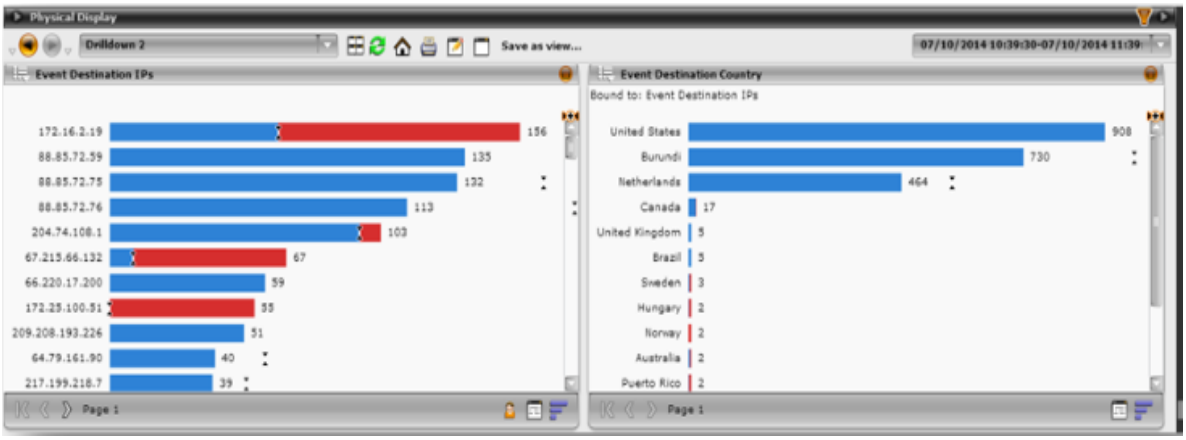
To de-select a binding filter, simply double-click in the whitespace of the source pane.

Filter by drilldown

Drilldowns allow you to take a source object (for example, a user, application, or IP address) and break it down into sub-groups by another field. To drilldown, simply select the one or more object you're interested in, and open the Drilldown menu to select a field to group them by. In our case, let's assume we're interested in knowing the breakdown of country associated with our malware events. We'll start with a Destination IP panel, pre-filtered to show our malware events. We'll select to drilldown by Destination Country (Event Drilldown/Geolocation/Destination Country).



When we make this selection, a new view is created on the fly (in this case, called "Drilldown 2"). This view starts with the Event Destination IPs pane where we made our original selection, and also incorporates the new Event Destination Country pane, which was our drilldown selection.



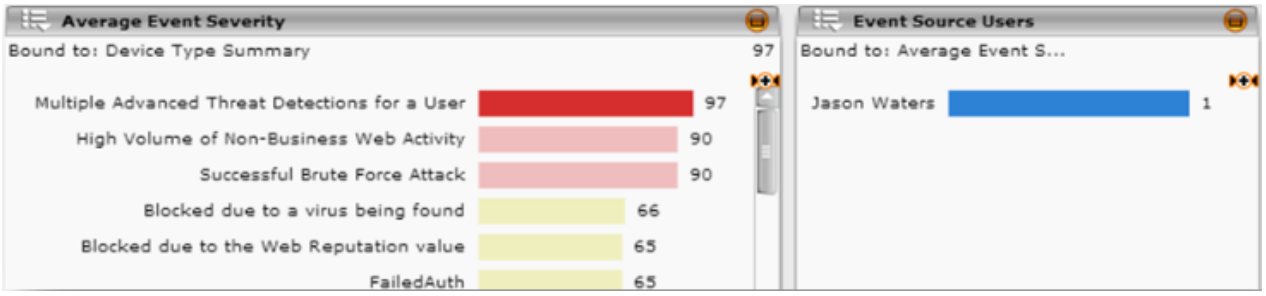
This new drilldown view acts just like any other view. It has integrated binding to link the drilldown groupings to the parent pane, and it supports filtering via any of the other options discussed above. You can add additional panes by performing additional drilldowns; each new pane will be automatically bound to the pane from which it was sourced.

If you would like to see your individual events, you can perform a drilldown to Events. This will provide you an Event Details pane you can use to explore events in fine-grained detail.

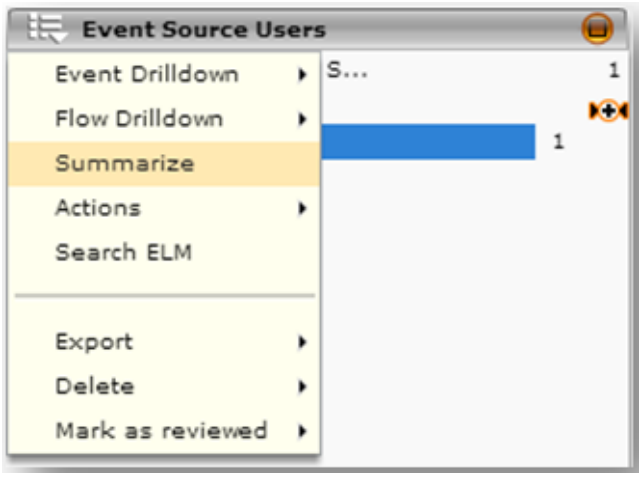
Summarize

Another tool that is worth learning early on is Summarize. Summarize provides the ability to "pivot" on an object of interest. It re-directs you to your pre-configured Summarize View (set per-user under options/Views), with a filter set in the Filter Panel to reflect the object of interest. Summarize is often used to get a higher level view of something that has caught your eye. For example, if you see a suspicious event associated with a particular user, you might summarize on that user to see all the related activity for that user over a selected timeframe.

Here we see a user associated with a malicious attack.



We'll select the user Jason Waters, and select Summarize from the popup menu on that view pane.



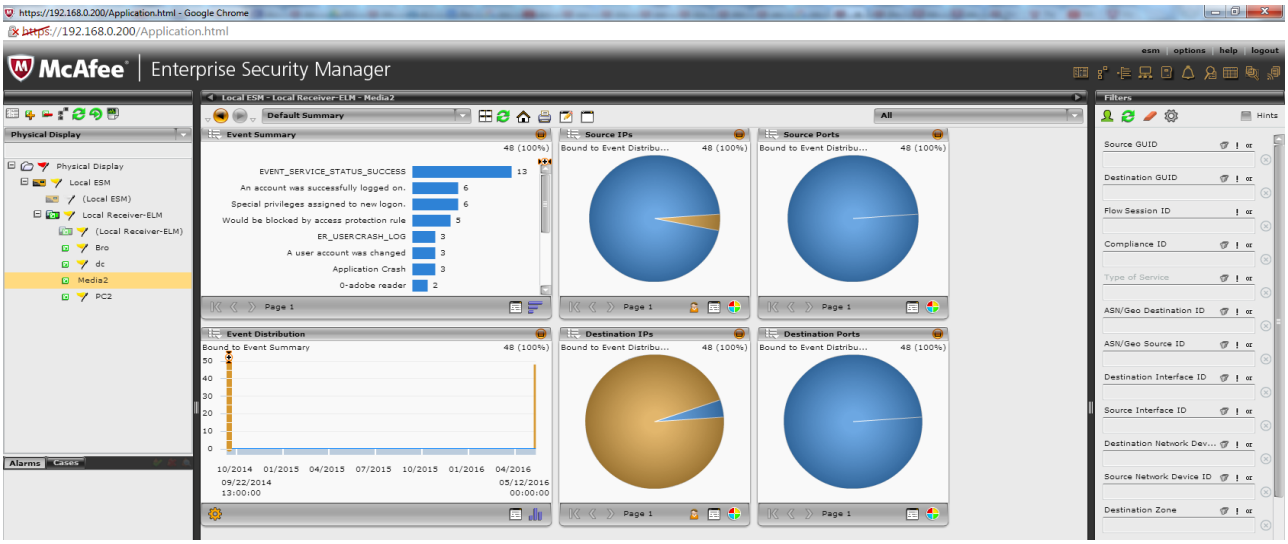
This brings us to our configured Summarize View, with a filter automatically applied based on the user we selected. We are now looking at all the events associated with Jason Waters over the timeframe we have selected. This gives us a bigger view of what Jason has been up to, and allows us to begin a detailed investigation.

A similar option to “Summarize” is “Look Around”. The Look Around menu option allows you to perform a time-based query to find events that occurred near to the selected event in time. When you choose Look Around, you are provided the option to apply optional filters to ensure you get only events that match specific criteria (for example, all events within 30 minutes that have the same source IP address).

Filter by Windows Event ID

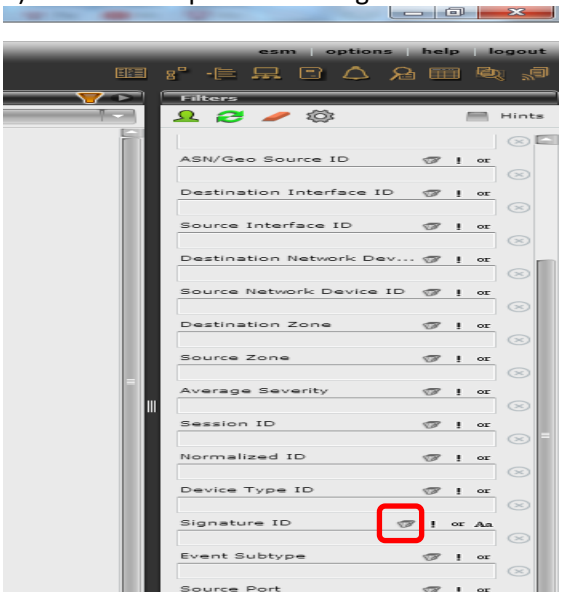
Being able to display exactly what you are looking for is key in using any SIEM. Without the capability, you could be wasting time sifting through logs to find what you need. Fortunately, ESM makes this task simple by being able to filter for specific criteria.

Let's say that we are presented with the below window when we log into the ESM. While this is only one workstation, we could become overwhelmed quickly is presented with more.

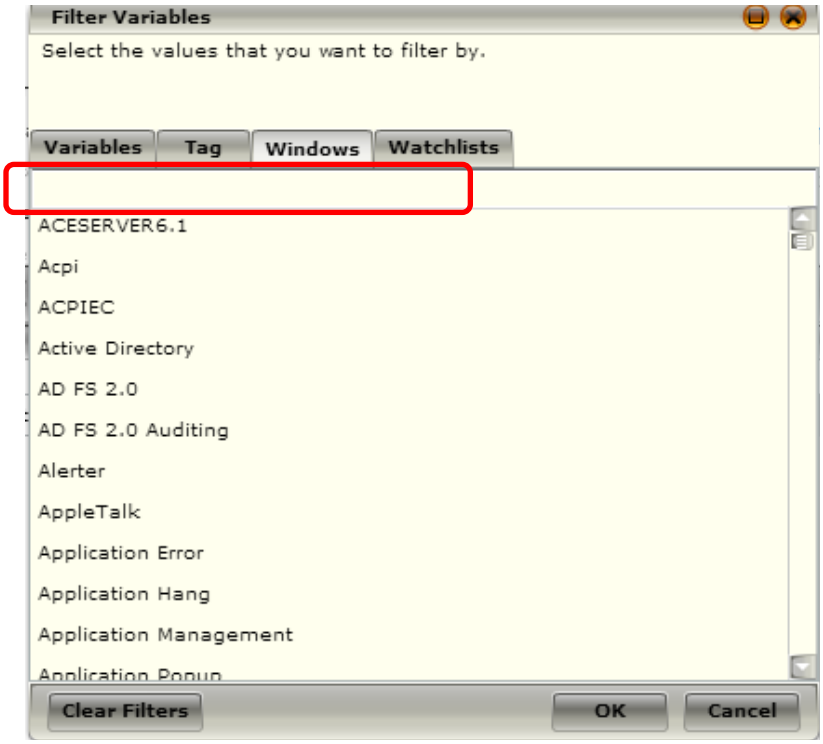


For this example, we will search for Event ID 4720 - A User Account was Created.

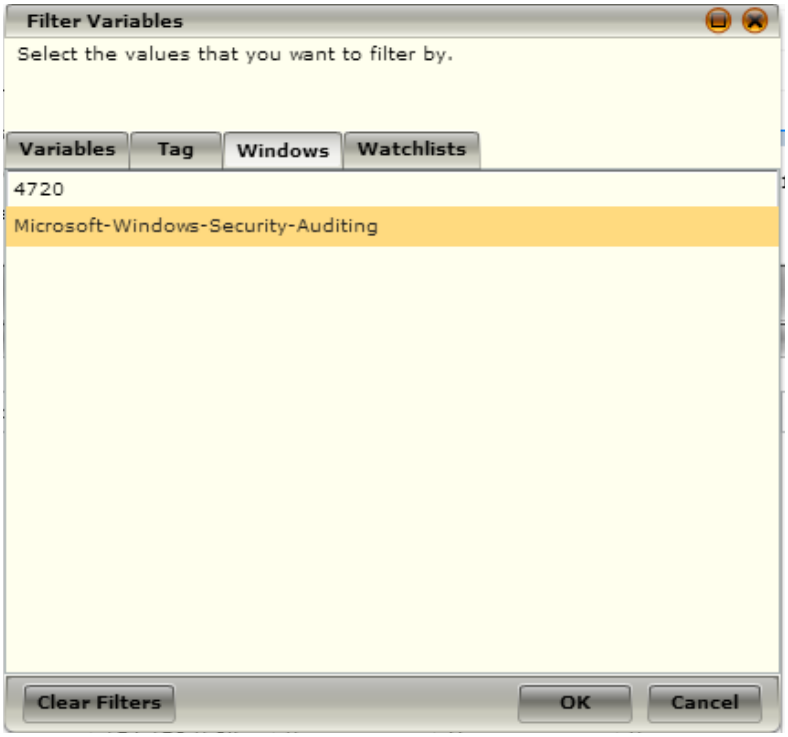
1) In the Filters pane on the right side of the screen, click the filter icon for "Signature ID".



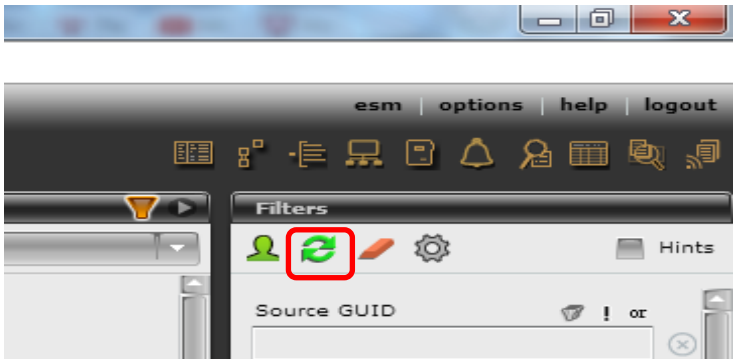
2) When the Filter Variables window appears, click the Windows tab.



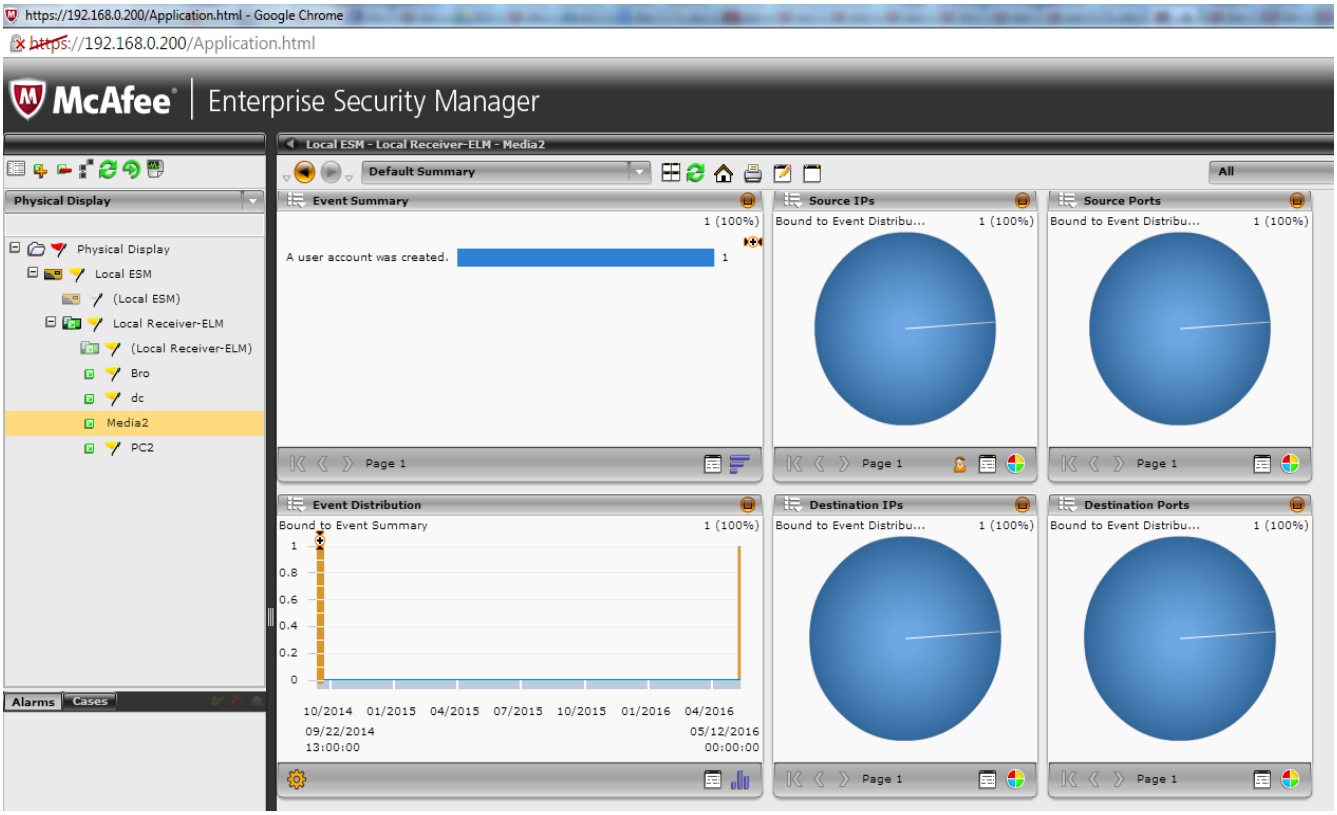
3) Input the Windows Event ID and "Microsoft-Windows-Security-Auditing" will appear... click Ok.
Note: "Microsoft-Windows-Security-Auditing" will be what comes up every time you filter for Event IDs.



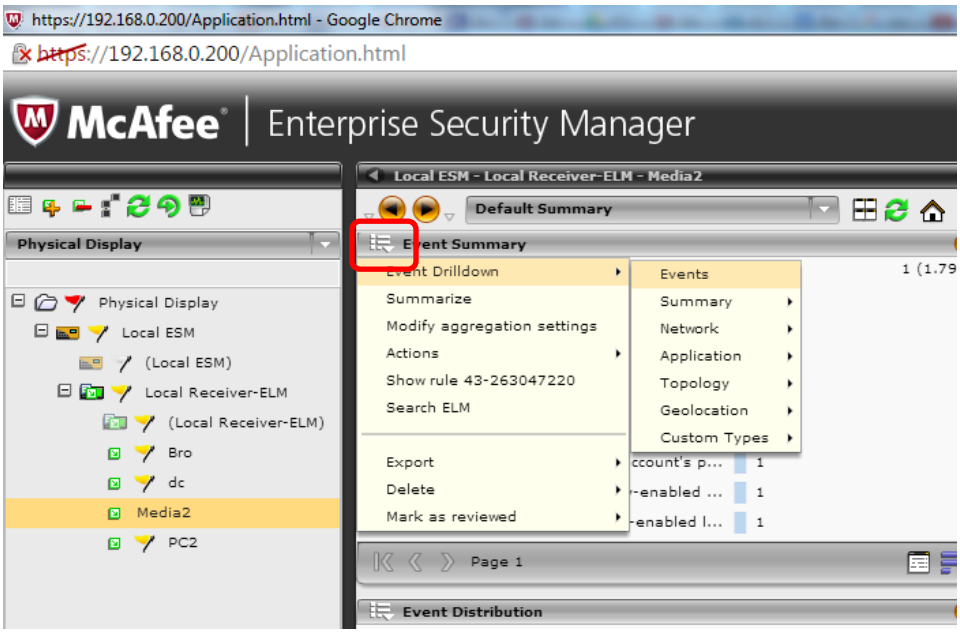
4) The filter for Signature ID will be populated with the specific filter.
5) Click the "Run Query" button to execute the query.



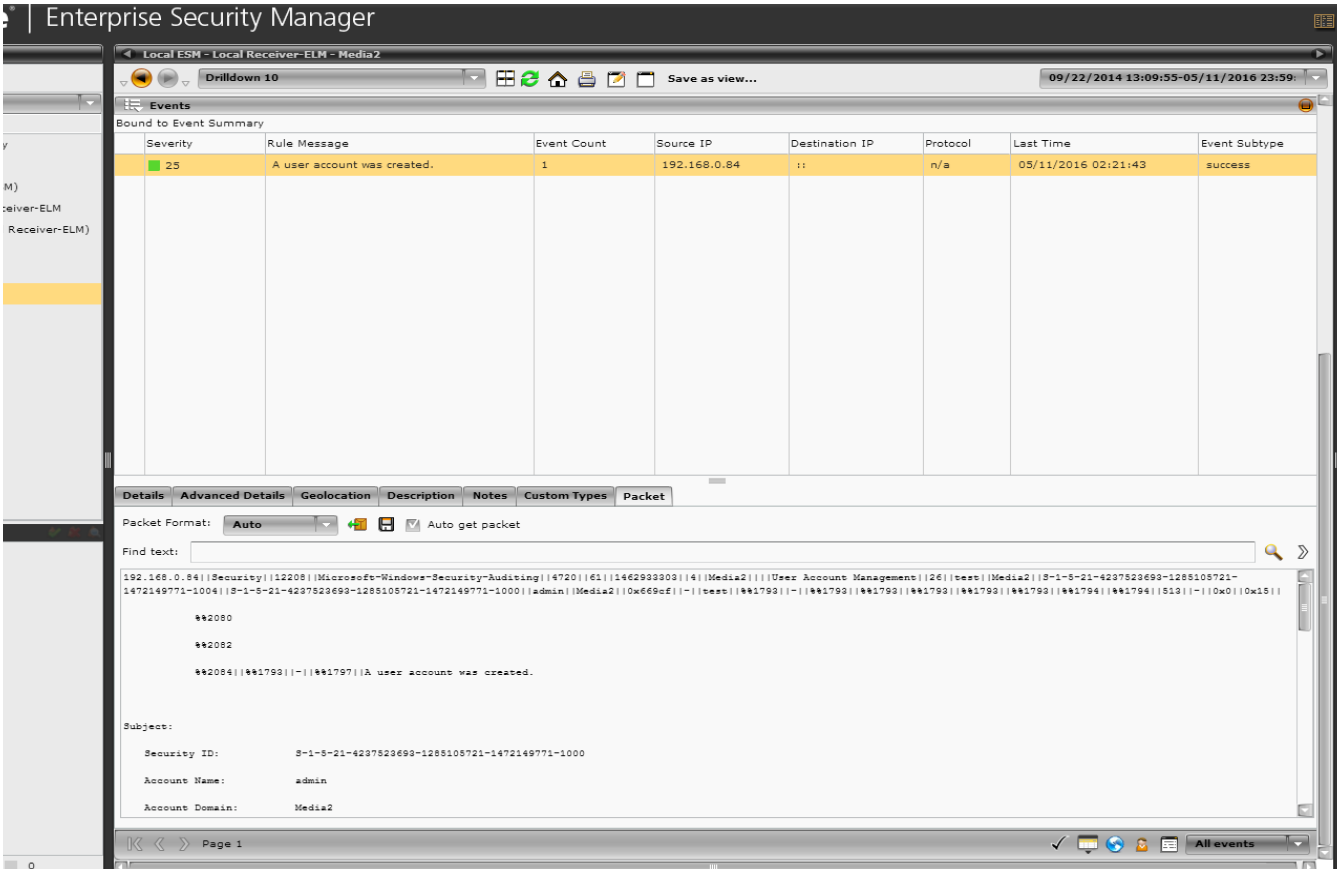
6) The entries meeting the specified criteria are returned. In our case, there is only one system.



7) We can drilldown and get more information on this entry, to do so, click the icon next Event Summary and select Event Drilldown > Event.



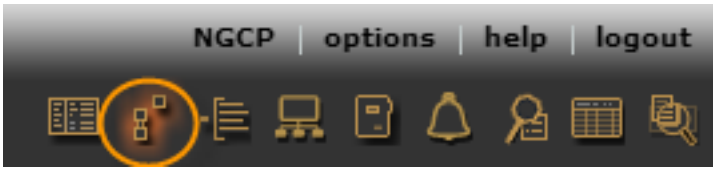
8) Click the event in the top pane. Down below, the packet will be displayed in the Packet tab. Other pertinent information is displayed throughout the other tabs. In the notes tab, one could actually input notes regarding the entry.



Variables Configuration

Variables are used by correlation rules in various ways to help identify suspicious and malicious behaviors in your environment. In order to be most effective, variables need to be configured to properly reflect your enterprise.

Variable definitions are configured in the Policy Editor. You can open the Policy Editor via the icon in the top-right corner of the UI.



The variables below provide a recommended list of variables that should be defined early in your McAfee SIEM deployment. Over time you may choose to tune other variables, or add new ones in order to optimize your SIEM deployment.

- Application/DAY_END
- Application/DAY_START
- Application/HOUR_END
- Application/HOUR_START

These variables allow you to define your standard working days and working hours. There are several correlation rules that leverage these variables to identify anomalous activities outside of standard working times. Keep in mind that the HOUR variables are defined in GMT time zone; you will need to convert your working time to GMT in order for these variables to be effective.

- Networks/HOME_NET

This legacy variable is used in place of the Local Networks/Homenet to identify internal IP addresses in some correlation rules. It should include the same IP ranges as Local Networks.

- Servers/DNS_SERVERS
- Servers/HTTP_SERVERS
- Servers/SMTP_SERVERS

These variables are used by correlation rules that identify anomalous activities related to specified protocols.

- Reputation/CORP_GEOS
- Reputation/SUSPICIOUS_GEOS

Corporate geographic location is typically defined as countries where your company has corporate offices. Suspicious geographic locations are typically defined as those where you would not expect to receive communication from during normal business operations.

Data Sources

Data Source Communication

By default, ESM blocks all IPs from communication to it until one of the following conditions has been met:

- A data source is created using a static IP
  Note: If using DHCP, you will need to also use the DHCP block option below.
- AutoLearning is enabled (basically disables the firewall for a period of time to allow communication)
  1) Receiver Properties > Data Sources > AutoLearn.
  2) Enable AutoLearn for a specific amount of time.
  3) Hit the refresh bottom and as systems appear, add them.
     Note: Used for syslog and SIEM Collector while systems are actively trying to contact ESM.
- Input the DHCP block
  1) Receiver Properties > Receiver/ELM Configuration > Interfaces.
  2) In the DHCP Block, input the network and subnet mask.

Adding Windows Event Logs Data Sources

One of the many great features of McAfee ESM is that it has the ability to pull logs from systems without any agent being present on the distant end. In order for that to happen, a data source has to be configured in ESM depicting the pertinent information about the system (host name, IP, logs to retrieve, credentials, etc.) so ESM is able to connect to the system and retrieve the specified information.

Data Source Methods

Configuring data sources for Windows event logs can be accomplished in one of a few ways. We will discuss the four most widely used methods here with recommended networks and/or reasons to choose the method. The methods are as follows:

- One data source at a time
  - Used for adding a few number of systems quickly
  - Can work using static IPs or DHCP
- Bulk data source import via a CSV
  - Used for to add a large number of systems
  - Does require some formatting of a CSV
  - Can work using static IPs or DHCP
- Importing data sources via Asset Manager
  - Requires access to Active Directory
  - Allows you to display all systems in Active Directory who are currently communicating with DNS
  - Provides an easy way to add data sources by highlighting multiple systems and adding them
  - Not ideal for DHCP networks
- SIEM Collector agent forwarding
  - Requires agent to be installed on remote system
  - Can be pushed out via HBSS (ePO), Group Policy, or something similar

- Must be configured to point back to ESM
- Works best for DHCP networks as it uses a Host ID to communicate
- Used as a way to get specific program logs (DNS, AD, etc..) while using one of the other three methods to grab the event logs

Prerequisites

- McAfee ESM version 9.3.2 and above for Microsoft versions 8.1, Server 2012-R2 and above.
- McAfee Enterprise Security Manager version 9.2.1 and above for Microsoft versions XP, Server 2003 and above.
- Administrative privileges on the Windows device.

Specific Data Source Configuration Details

In order to pull event logs from a system, the following type of user account is needed.

1) For Windows XP, Server 2003 and above create a user account added to the Administrators Group.
2) For Windows 8.1 and Server 2012 R2 use the Administrator user account or create a user account added to the Administrators, Distributed COM Users, and Event Log Readers groups.

Note: If using the latter option, you must configure the data source to use RPC.

Adding a Data Source (one a time)

One of the many great features of McAfee ESM is that it has the ability to pull logs from systems without any agent being present on the distant end. Setting up ESM to pull event logs from a Windows based system come be accomplished utilizing the following:

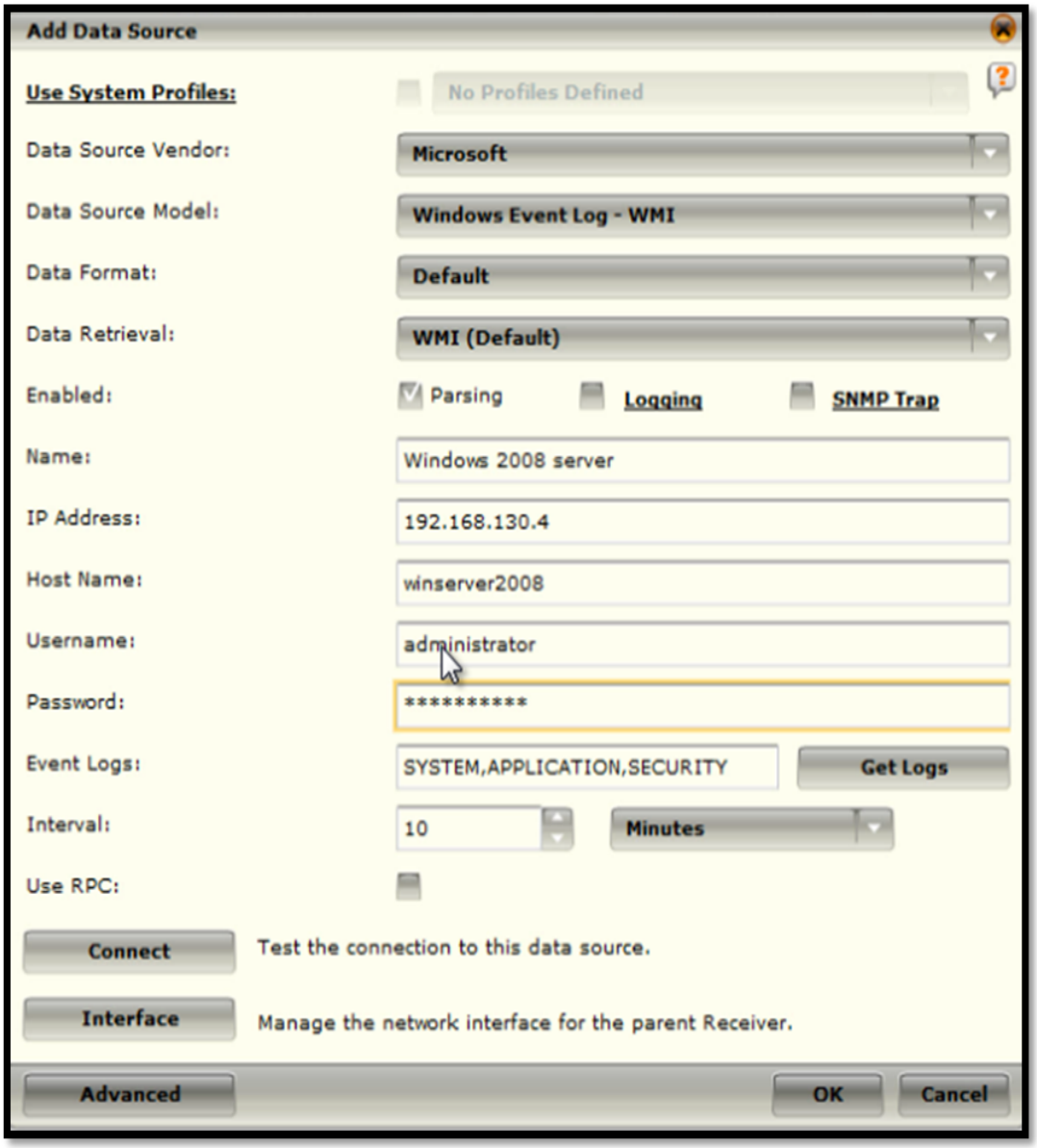
1) Once logged into ESM, expand your Local ESM in the System Tree on console on the left side of the screen.
2) Click on the Event Receiver and then click Add Data source in the top left corner of the console.

3) When the Add Data Source screen appears, complete the following fields with the specified data:
    - For data source Vendor, chose Microsoft.
    - For the data source Model, the options available to you will vary depending on the vendor you picked for the data source vendor. In our case, we picked Microsoft, so we are presented with Microsoft related options. Here, we are going to pick WMI Event Log.
    - Leave the Data Format and Data Retrieval to Default.
    - Now we have the option to check a “parsing” and a “logging” checkboxes. “Parsing” means that the logs will be parsed and inserted into the ESM database. “Logging” means the logs will be sent, raw and unparsed, to the event log manager component. The options you chose depend on your specific needs. In our particular case, we are going to leave parsing checked.
    - Provide a Name: This is how this data source will appear in the SIEM system tree. You can pick any name you want.
    - Enter the IP address of your windows system. If you are using DHCP for your Windows system, starting at version 9.4, you don’t need to enter an IP address, you only need to enter the host name in the next box.

        Note: If relying on DNS to resolve a hostname with a DHCP address, ensure that ESM is configured with the DNS IP address. To do so navigate to Properties > Network Settings. Under the Main tab, click Setup next to an Interface. When the window opens, input the DNS server IP.

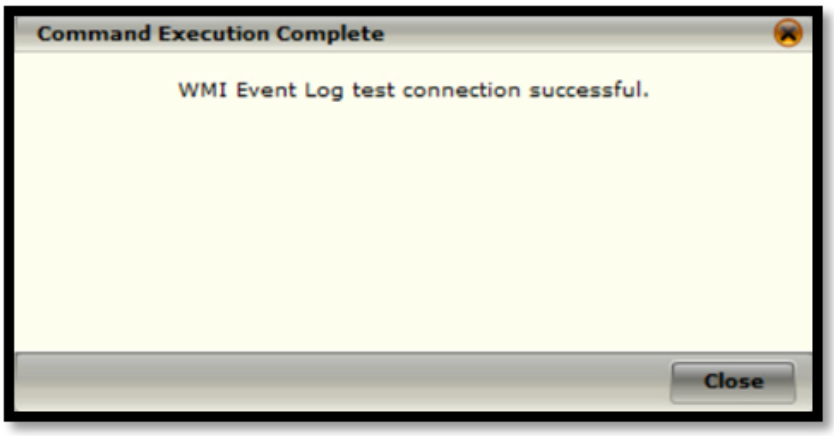
    - Enter the host name of your Windows system.
    - Fill in the username and password of an account with administrator rights.
    - Under Event Logs: APPLICATION, SYSTEM, SECURITY – By default, the Receiver will collect security, administration and event logs. You have the ability to enter other log files, such as Directory Service or Exchange if this is a Windows server is running those services. The event log data gets collected in the packet data and can be viewed through the event table details. If you enter additional logs, make sure there are no spaces between the log names.

- The next setting, Interval, determinates how often the Receiver will check windows logs for new events. Generally, 10 minutes is a good rule of thumb for windows servers and anywhere from 5 to 10 minutes for workstations. The environment in which you operate in will influence your decision on how often ESM should pull logs.



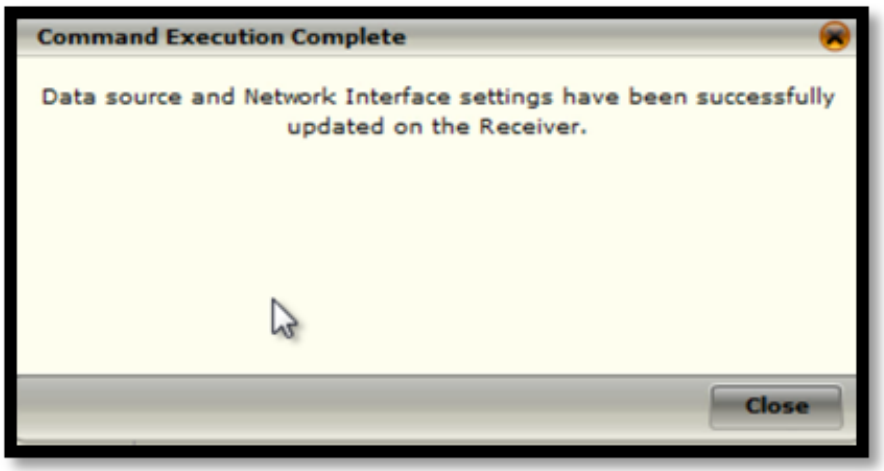
4) Click Connect to test your credentials.

5) A test connect successful message appears. Click Close. Then Click OK to close the Add Data source window.



6) The Apply Data Source Settings pop up appears. Click yes so your receiver is updated with the new Windows WMI log data source that you just created.

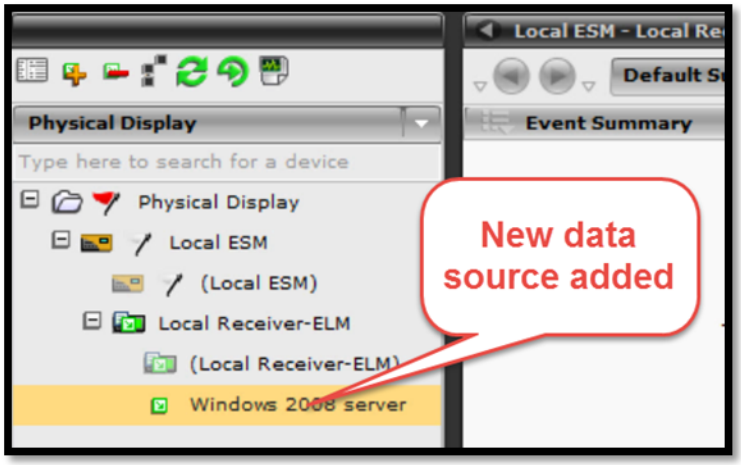
7) An update is successful pop-up appears when the update has been successfully applied. Click Close.



8) The Policy Rollout screen automatically opens. This is to ensure that policies are immediately rolled out within ESM. Notice that the data source you just created is listed. Click Ok and the rollout will begin on the newly added system. Other systems that were previously added and are

listed here will be skipped automatically since the policy is already applied for them. The window will close by itself when the task is complete.

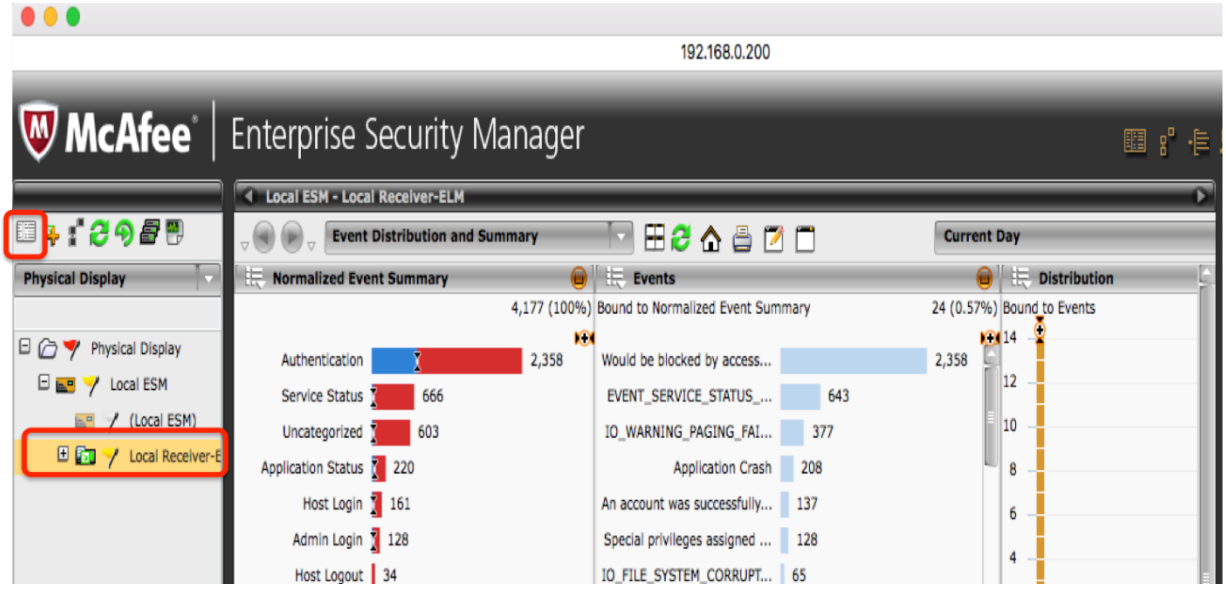
9) The newly added system is now present in the System Tree.



Bulk data source import via a CSV

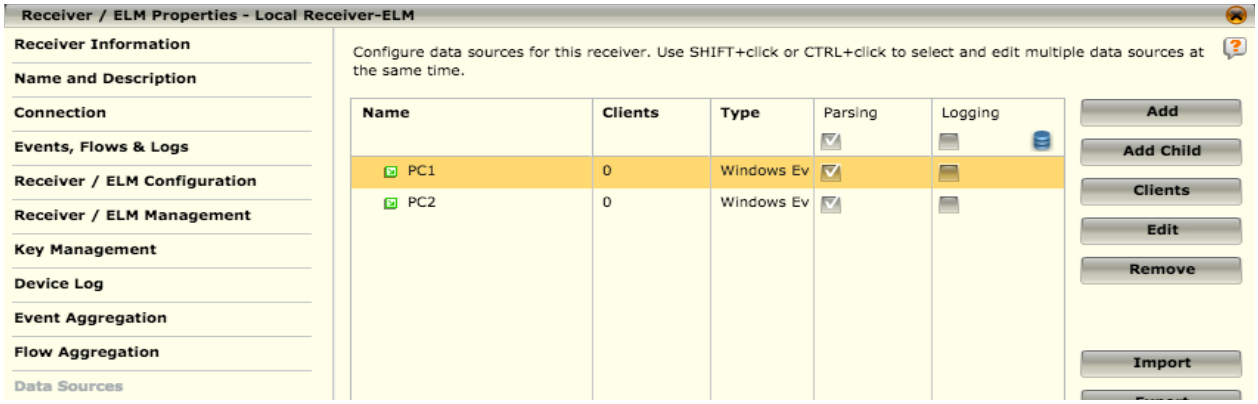
Importing data sources from a csv allows for multiple data sources to be configured at one time. When importing sources, there is a very specific format that ESM is looking for. It is possible to export a data source from ESM in order to get the format but we have created a PowerShell script do all the work for us. The script can be found in Annex A of this document. To use the script, do the following:

1) Get the Device ID from the Receiver Properties > Name and Description.

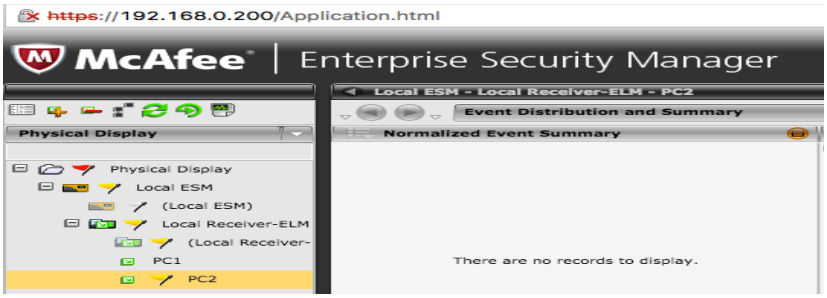


2) Open PowerShell and execute the esm_import.ps1 script (Annex A).

3) Input the Device ID of ESM, credentials that will be used to authenticate the end workstation, and select the suitable options when prompted.
   Note: The csv will be saved to the location in which the script is run from.
4) Once complete, open the csv with Notepad or Notepad++ and save the csv with UTF8 encoding.
   Notepad: Click Save As and hit the dropdown to change the encoding to UTF8.
   Notepad ++: Select Encoding from the toolbar and select UTF8.
5) To import the csv, open the receiver properties again as noted in step 1 above.
6) Click Import.
7) Click Choose File.
8) Click Upload.
9) Create one data source using the method above which will serve as a template for us to use.
10) Navigate to the properties of the receiver as shown below.
11) Click Import.
12) Browse to the csv file and select it.
13) Click Upload.
14) A window will appear showing what systems will be imported and their settings.
15) Click Ok.
16) The number of data sources to be imported will be listed.
17) Click Close.
18) Click Cancel
19) The newly created data sources will be listed as shown below.



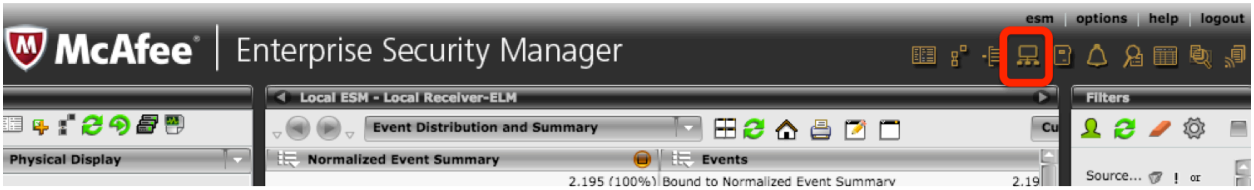
20) Click Ok to close the window.
21) Click Yes when prompted to add the changes to the receiver.
22) Click Ok to rollout the changes to the receiver.
23) Click Close to acknowledge the data source being successfully added to the receiver.
24) The newly imported data sources will now appear in the receiver tree as shown below.



Importing data sources via Asset Manager

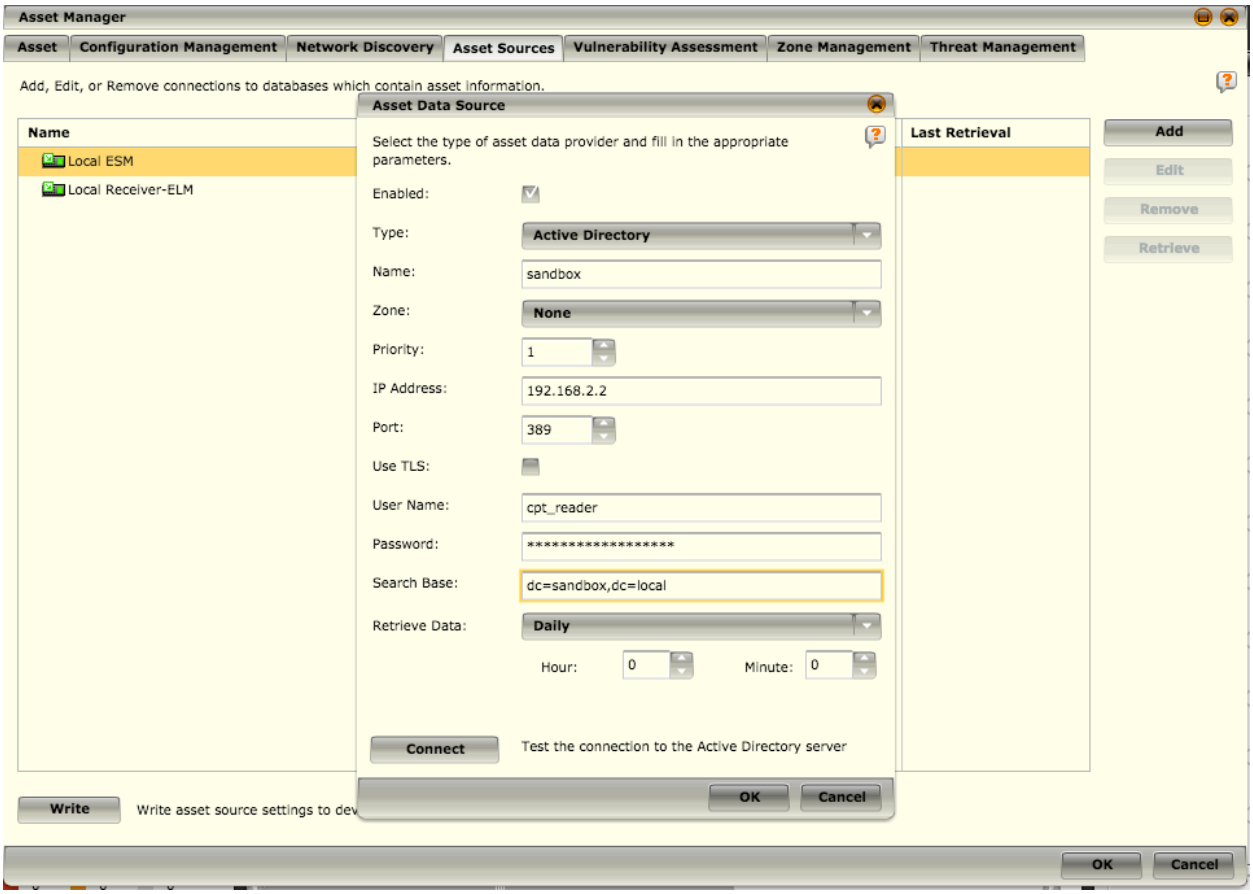
Asset Manager provides a centralized location that allows us to discover, manually create, and import assets from Active Directory.

1) Click on Asset Manager.

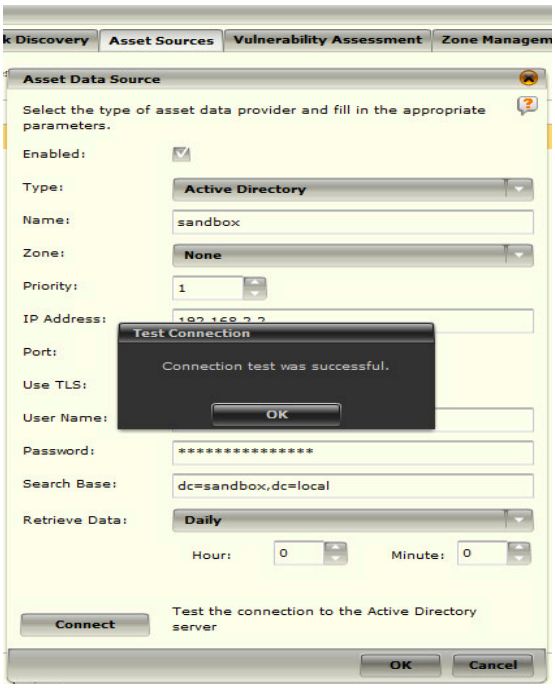


2) Click the Asset Sources tab.
3) Highlight ESM and click Add.

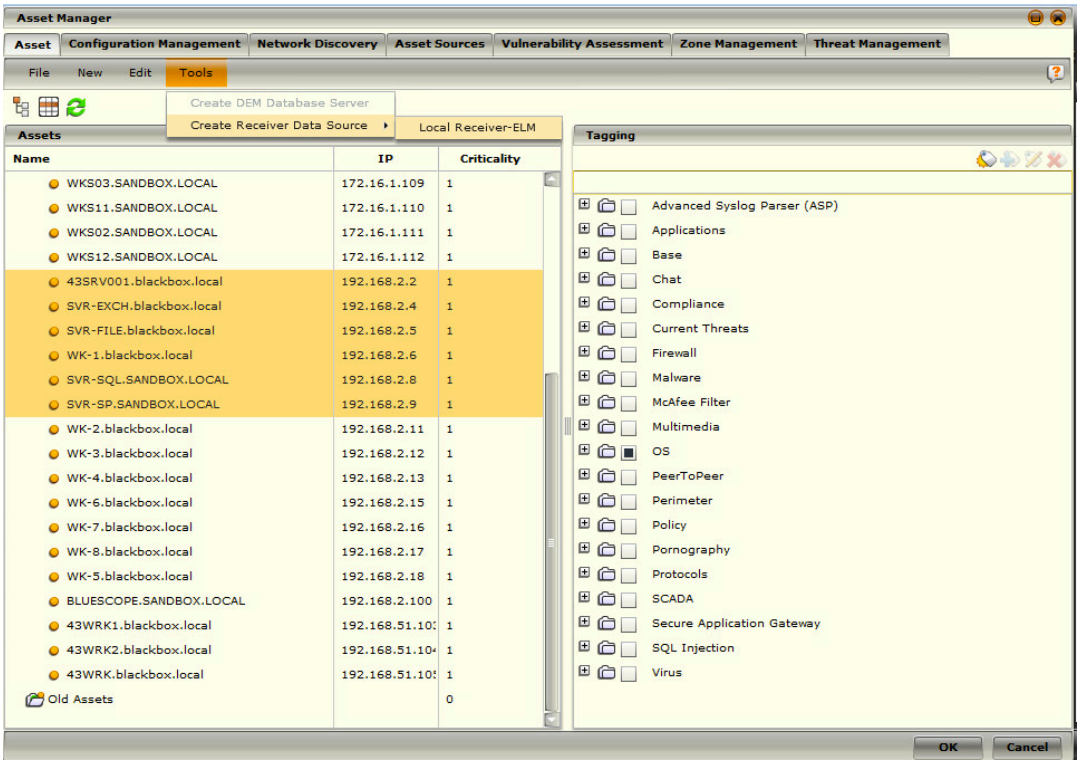
4) Input the requested information and click Connect in the bottom left of the screen to test the connection.



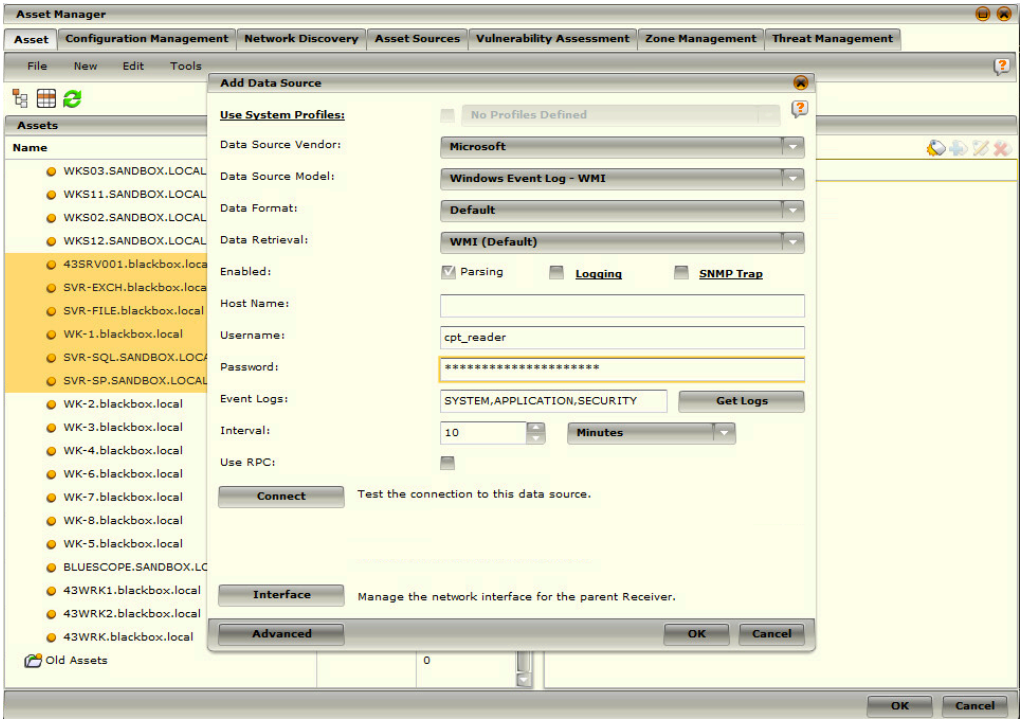
5) Click OK upon successful connection testing and click OK again.



6) Click the Write button in the bottom left corner to write the settings to the device.
7) When the status in the pop-up window says “Success”, click close.
8) Highlight the newly added Active Directory source and click retrieve.
9) Click OK once the data retrieve is complete.
10) Click the Asset tab.
11) Expand Unassigned.
12) Highlight all the systems you want to add as data sources.



13) Click tools > Create Receiver Data Source > Local Receiver –ELM.
14) Input information as shown below.



15) Click OK.
16) Click Yes.
17) Click close.

18) The data sources will now show up in the receiver tree.

SIEM Collector Agent Forwarding

The McAfee SIEM Collector is host-based software that can be configured to send events to a McAfee ESM with a Receiver. The SIEM Collector can be configured to send events from the local Windows machine or from remote Windows machines.

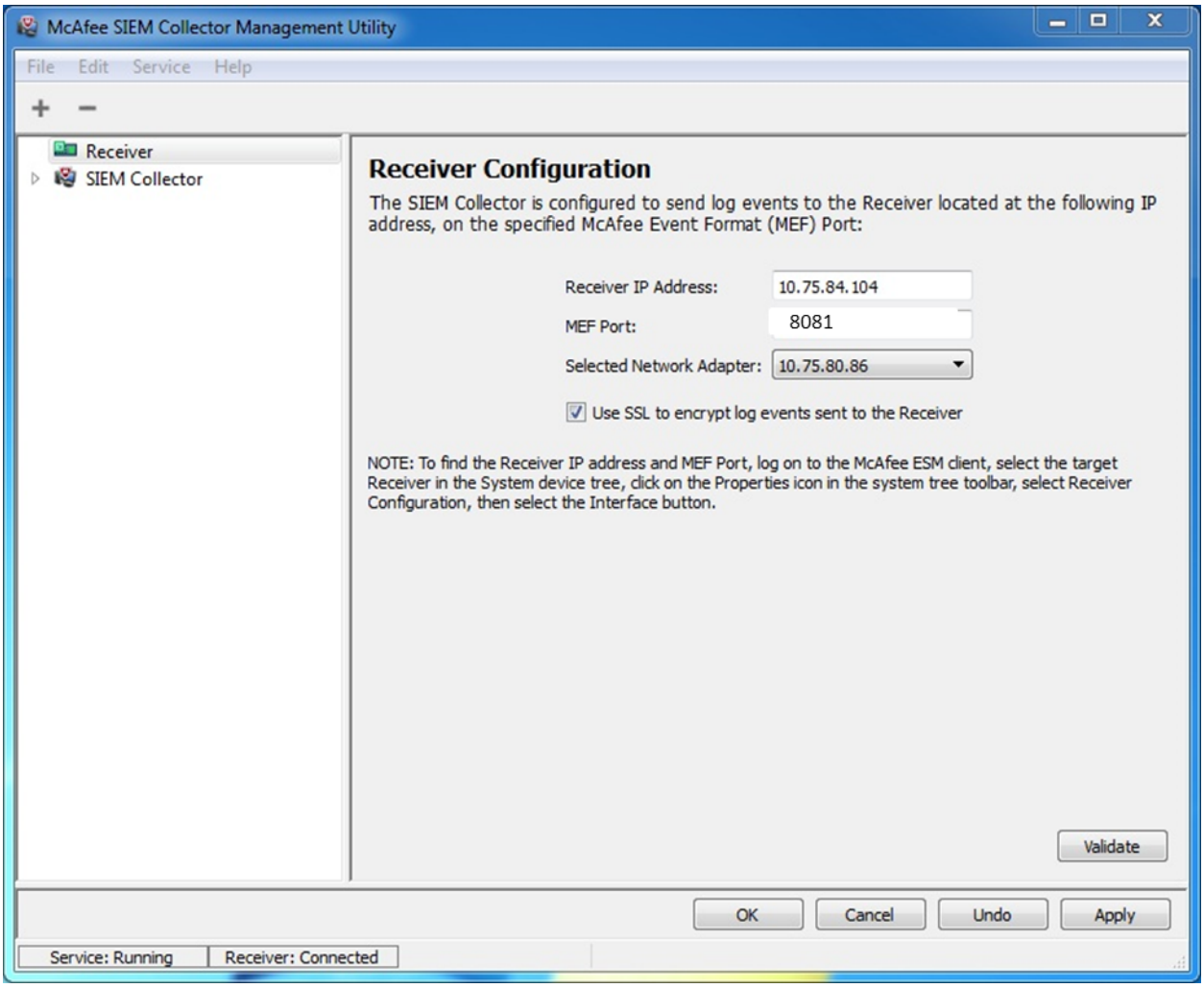
It is also possible to deploy the SIEM Collector from HBSS (ePO) and do the configuration from there as well. We will address here how to do a single system.

SIEM Collector Installation

1) Obtain the SIEM Collector software from someone with access to the McAfee client portal.
2) Double-click the executable.
3) Click “I Agree”.
4) Confirm your installation directory and click “Next” to continue.
5) Read the installation overview and click “Next” to continue.
6) Type in the IP of the Receiver and change the port to 8081.
   Note: If you choose to encrypt, you must select that option on ESM as well
7) Click Next.
8) Click Finish.

SIEM Collector Receiver Settings

To change the settings of the Receiver that the SIEM Collector communicates with, open the SIEM Collector configuration utility and select the appropriate Receiver.



When the Receiver node is selected, the screen displays information regarding the Receiver to which the event data is being sent. This includes the Receiver's IP address (must be a valid IP address), MEF port, and the Network Adapter to use. It reflects the information that was entered when the Utility was installed.

If you don't know the target Receiver's IP address or MEF port, do the following to locate them:

1) Log on to the ESM console.
2) Select the node of the target Receiver in the Navigation Tree.
3) Click on the Properties icon in the Actions Toolbar. The Receiver Properties screen will open.
4) Select Receiver Configuration.
5) Select Interface. The IP address and MEF port will be listed on the screen.
    - MEF Port: This port value should be the same as the MEF Port that the Receiver is configured to use.
    - Selected Network Adapter: If you want to select a specific network adapter to be used for communicating with the Receiver, you can select it from this list.

Using SSL to encrypt log events sent to the Receiver:

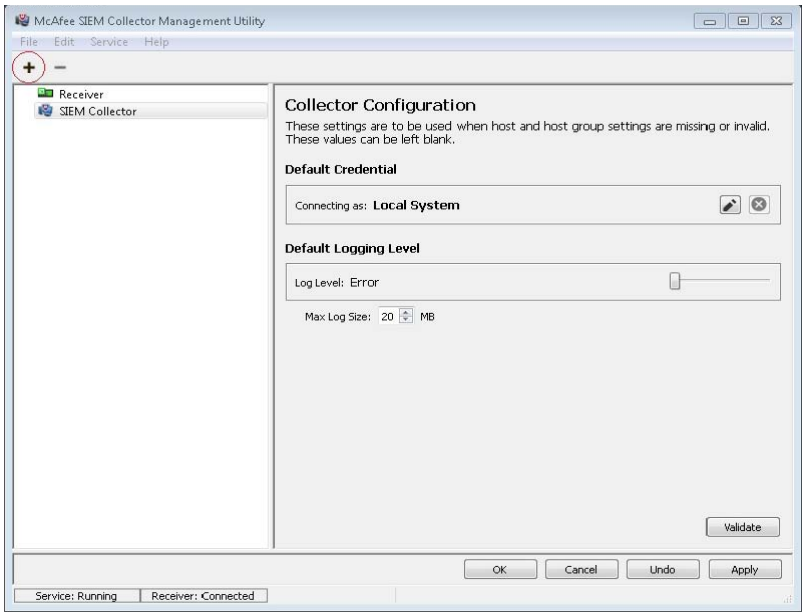
If you want the event logs to be encrypted using SSL, this box should be checked. (See Clients section for more help with encryption and encryption with host IDs).

Whenever a change to one of these fields is made, click Apply to save the changes and keep the Utility open or click OK to save the changes and close the Utility. Clicking either of these buttons validates settings and restarts the service if it is running.

Group Configuration

1. Launch the McAfee SIEM Collector Management Utility by navigating to Start > All Programs > McAfee > SIEM Collector Management Utility.

- Select the "Receiver" node in the tree view on the left-hand side of the interface, and confirm the Receiver IP address and port value. Make changes as necessary.
- Select the "SIEM Collector" node in the tree view. Click on the plus sign above the tree view to add a new host group.



- A host group is a container object that will contain hosts. One or more hosts can be added to a group to ease management of a SIEM Collector configuration that will remotely collect events from many hosts.
- Once you have clicked the "Add Group" button, a host group object will be created, and the properties of the host group will be displayed in the right-hand panel. New groups are marked as Disabled by default. A group must be enabled to collect from any hosts under that group.
- On this screen you can change the name of your new host group and the credentials that will be used for collection. Click "Apply" to save changes.
- Credentials may be set at the Groups level and inherited by all child nodes in the group Individual nodes can be changed to not use the group's credentials if desired.

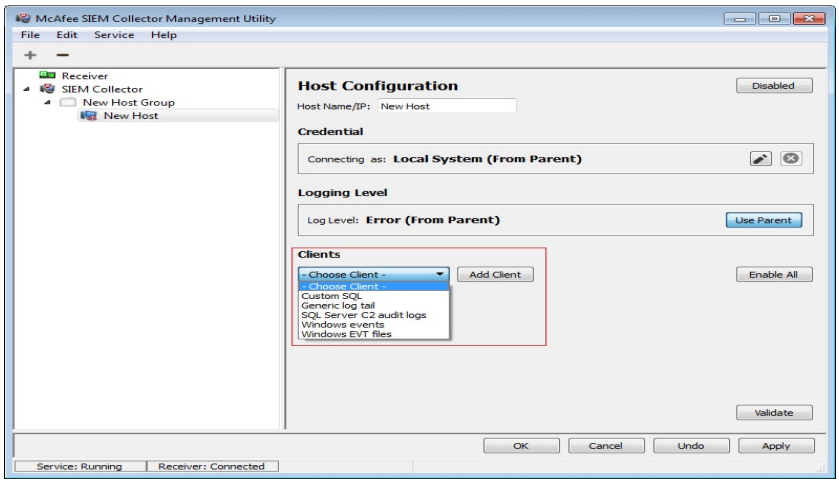
Note: Credentials are only validated when the group has enabled clients. Failed validation will disable the client/host.

- The logging level may be set for the selected group. This setting is inherited by all of the group's child nodes. Individual child nodes may be changed to not use the parent's settings.
- With the host group selected, click the plus sign above the tree view to add a new host.

- On the host properties screen on the right, type in the DNS name or IP address of the host you will be collecting events from.
- The Host is disabled state by default. The host must be enabled to collect from any of its clients.
- Credentials are inherited from the parent group but may be over written.

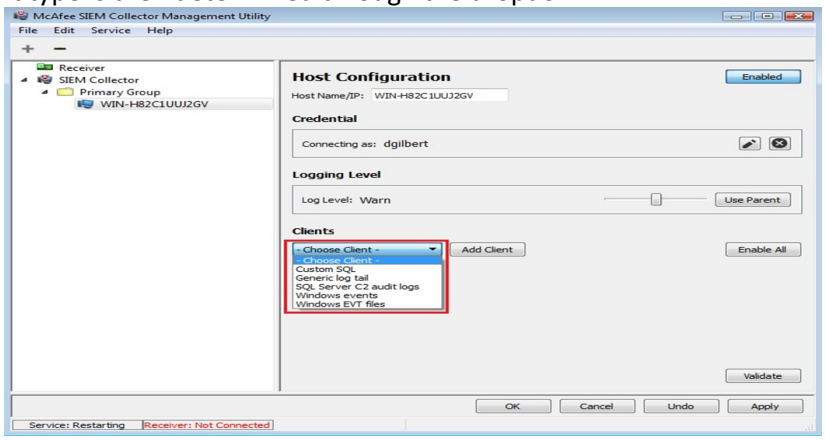
Note: Credentials are only validated when the host has enabled clients. Failed validation will disable the client/host.

- The Logging Level is inherited from the parent group but may be over written.
- Encryption settings are automatically established based on what the Receiver datasource is configured with.
- To add a new client, select a client type from the "Choose Client" drop-down box and then click "Add Client".



Clients

When adding a client, you must first select the Host that you want to add the client to. The client type is then determined through the dropdown:



ENCRYPTION

Enabling encryption with SSL between the SIEM Collector and the ESM requires **both** devices to have it enabled.

ENCRYPTION WITH HOST IDS

In order to use encryption with host IDs it must be set up with one 'bridging' client that uses an IP address. This opens the firewall for the connection and allows the receiver to connect with an encrypted connection.

Custom SQL

For collection from both MSSQL and Oracle databases, if the database credentials are not the same as the credentials of the machine on which the database resides, the database credentials will need to be entered in the "Credential" section of the "Host Configuration" screen.

Installing Drivers

Oracle

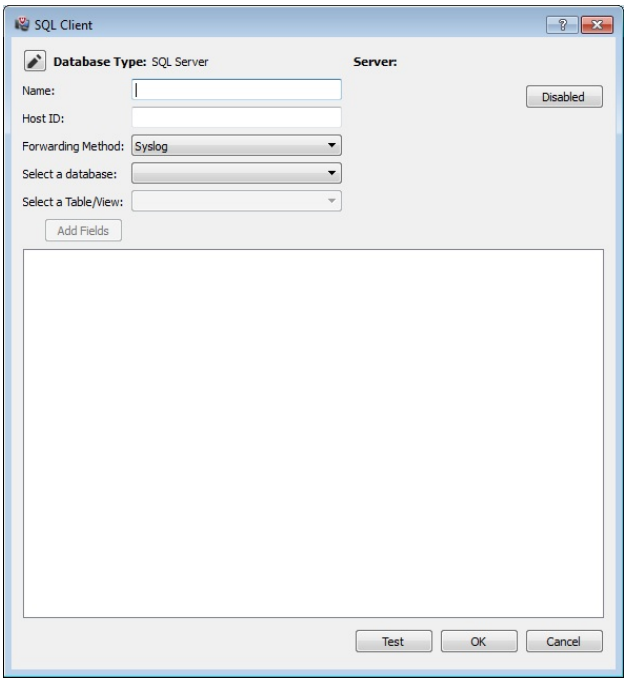
- Download the Instant Client Package - Basic version 11.2.x.x
- Create a folder under C: called instanclient and un zip the drivers into the new folder
- Open Control Panel -> System and Security -> System
    - Open Advanced system setting
    - Open Environment Variables...
    - Add "C:\instantclient;" (no quotes) to the path Environment Variable.

MSSQL

Install Microsoft® ODBC Driver for SQL Server.

Note: This will be different depending on your Windows version.

After configuring the database credentials, select "Custom SQL" from the client drop-down list and press "Add Client". On the "Login to Database" screen as pictured above, the database type and security can be selected. "Security" can be either "Windows Integrated Security", meaning the client will use the Windows account credentials for the host as configured in the "Credential" section; or "Database Security", meaning the client will use the database credentials as configured in the "Credential" section. Windows Integrated Security authentication is currently only available for SQL Server connections.



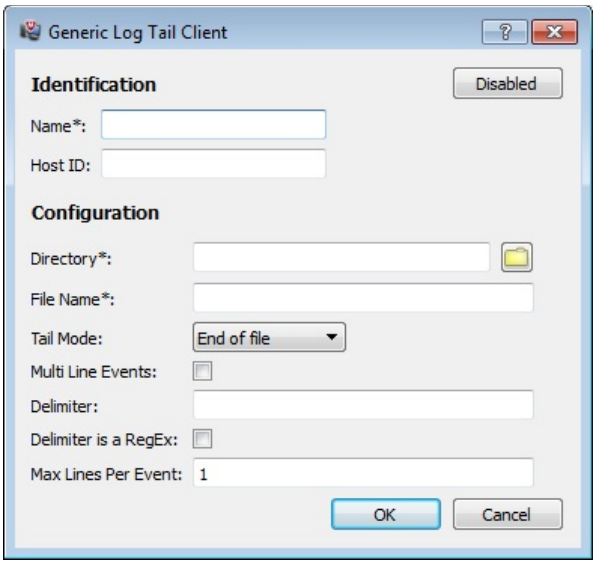
Note: The bookmark field is used to determine which record in the table is used to track where the last collection ended. Initially the bookmark is set to the latest record in the table; only records after this point are collected.

After configuring the login details, the "SQL Client" window appears. On this screen, the following fields can be configured:

- Name - Required. The name of the client.
- Host ID - An ID that corresponds to a host ID associated with a data source on the Receiver.
- Forwarding Method - Determines if the events are sent as syslog over MEF or field mapped as MEF.
- Select a Database - Lists the databases available to collect from.
- Select a Table/View - Lists the tables available to collect from in the selected database.

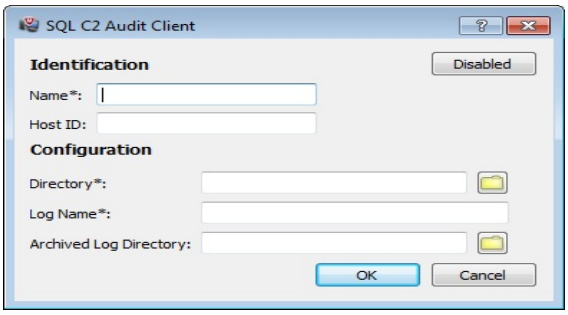
After selecting a database and table to collect from, a column must be selected to be used as the bookmark, and columns must be selected to collect from. If "syslog" is selected as the forwarding method, no further configuration is needed. If "MEF" is selected as the forwarding method, the database columns must be mapped to MEF fields. "Message" is the only required MEF field and must be mapped to a column in the selected table.

Generic Log Tail



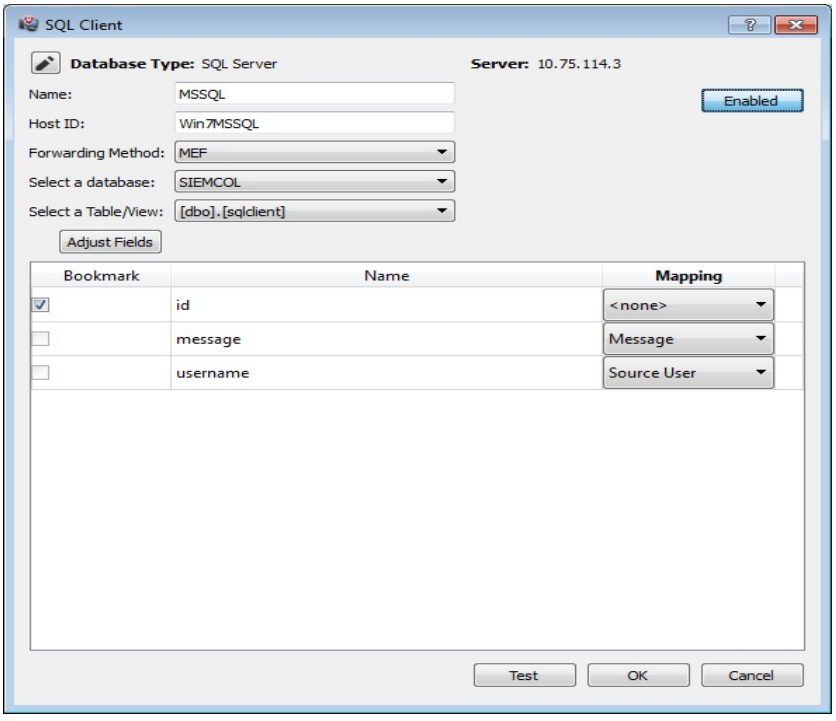
- Name - Required. The name of the client.
- Host ID - An ID that corresponds to a host ID associated with a data source on the Receiver.
- Directory - Required. The path that the client will pull log files from. The directory field can be entered manually, or the file browser can be used to navigate to a path by clicking on the folder icon.
- File Name - Required. The name of the file that the client will read. This can be a full file name (i.e. "dhcp.log"), or use wildcards (i.e. "*.log" or "*").
- Tail Mode - Determines whether the client will start reading the log from the top of the file or start from the bottom with new events as they are written to the file.
- Multi Line Events - Used to indicate whether or not the events in the log file span multiple lines or not. Setting this field will require setting a delimiter.
- Delimiter - Determines what the client uses as the delimiter between events (i.e. "Linux" would split the events whenever the word "Linux" is found, and "(?:\d{1,2}\/){2}\d{4}" would split the events every time a date in the format MM/DD/YYYY is found). Leaving this field blank will default to delimiting on newlines.
- Delimiter is a RegEx - Indicates whether or not the delimiter in the "Delimiter" field is a regular expression.
- Max Lines Per Event - Indicates the maximum number of lines a multi-line event can span.

SQL Server C2 Audit Log

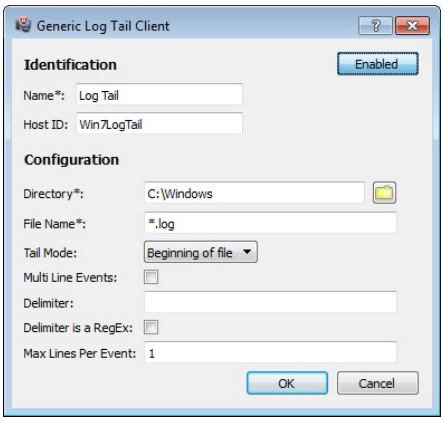


- Name - Required. The name of the client.
- Host ID - An ID that corresponds to a host ID associated with a datasource on the Receiver.
- Directory - Required. The path that the client will pull log files from. The directory field can be entered manually, or the file browser can be used to navigate to a path by clicking on the folder icon.
- Log Name - Required. The name of the file that the client will read. This can be a full file name (i.e. "logs.trc"), or use wildcards (i.e. "*.trc").
- Archived Log Directory - If a value is entered, the log files will be moved to this directory after being read.

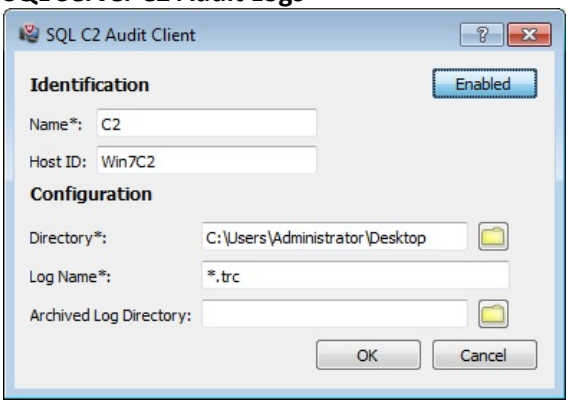
Sample Windows Client Configurations
Custom SQL



Generic Log Tail



SQL Server C2 Audit Logs



ESM DATA SOURCE CONFIGURATION

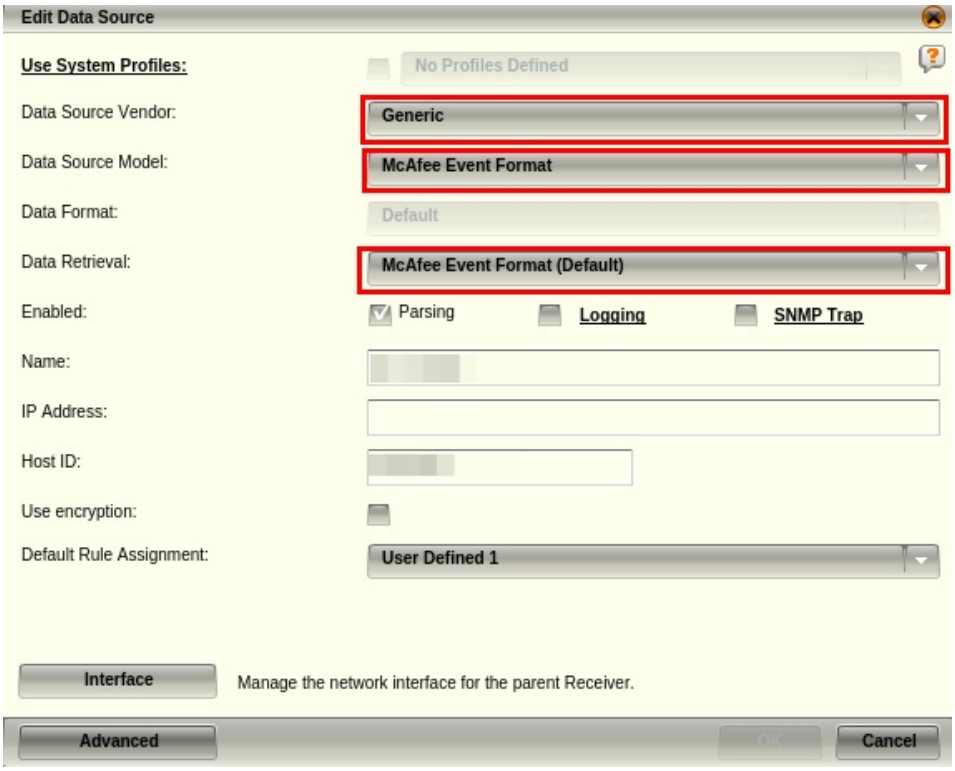
The ESM data source type will depend on which SIEM Collector Client type is chosen to collect from.

Important: If your SIEM Collector is collecting logs from other sources you must create an ESM data source for that IP Address. Or use the DHCP mask and host IDs.

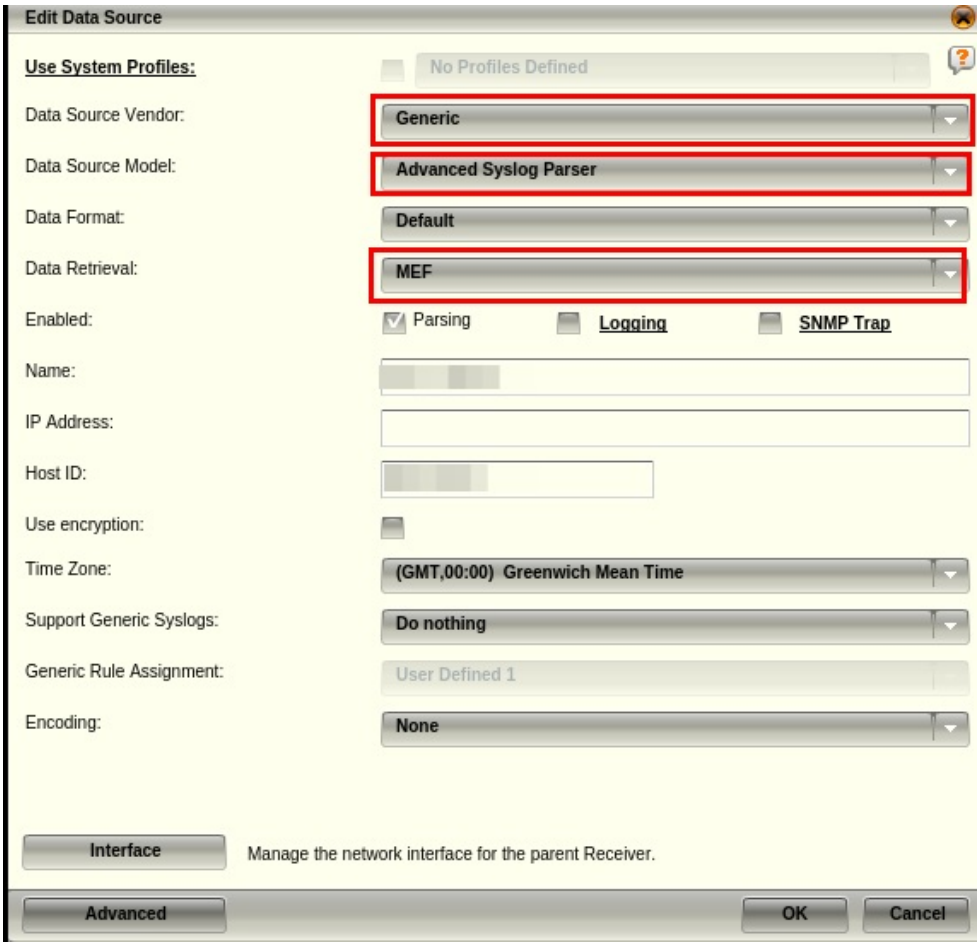
Note: If a Host ID is used on the SIEM Collector then the ESM data source may use the Host ID instead of an IP Address. (See the Clients Encryption with host IDs section for using this host IDs with encryption).

Custom SQL

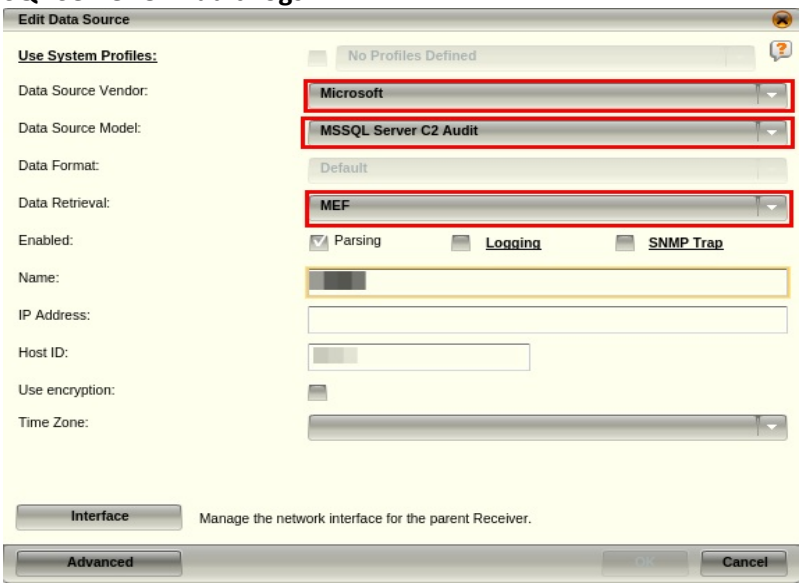
Note: The Generic SQL may also be set up as a Generic Syslog data source.



Generic Log Tail



SQL Server C2 Audit Logs

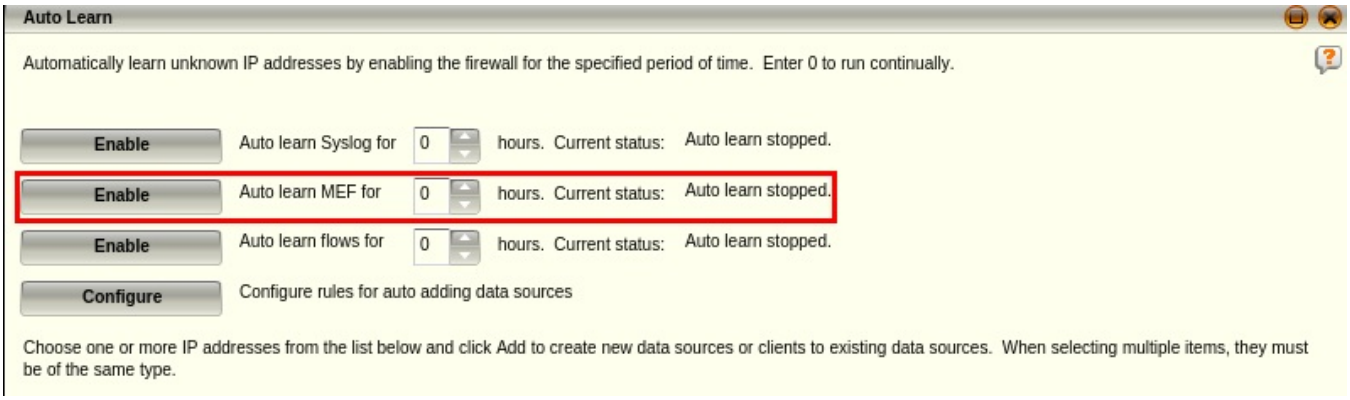


AutoLearn

See AutoLearn documentation to setup AutoLearning. Custom SQL may also use Syslog as the Autolearn type.

To access AutoLearn,

1) Open Receiver Properties.
2) Select Data Sources.
3) Select AutoLearn.

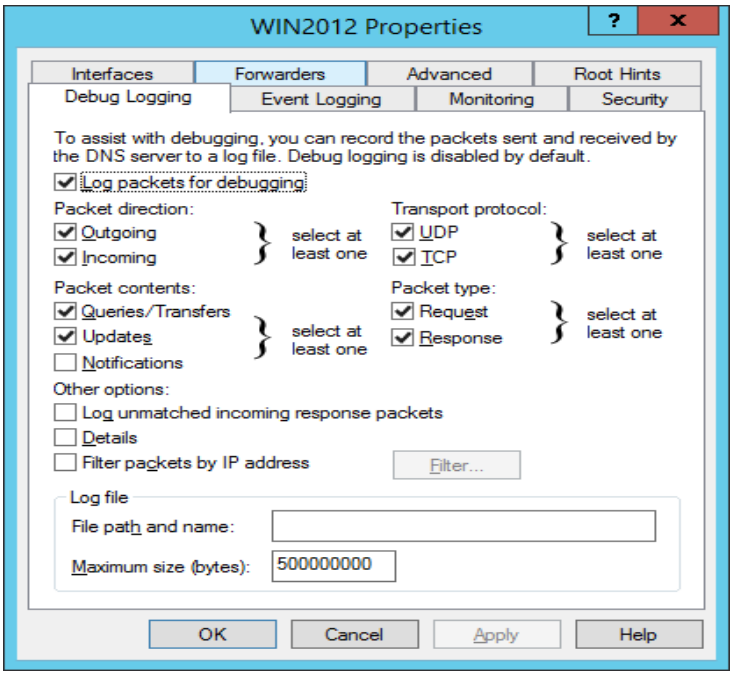


Adding DNS Data Source

DNS logs are an excellent source of data within an organization. It can be automatically correlated with other threat intelligence within the McAfee ESM and provide alerts when suspicious activity is detected. To set up the data source, do the following:

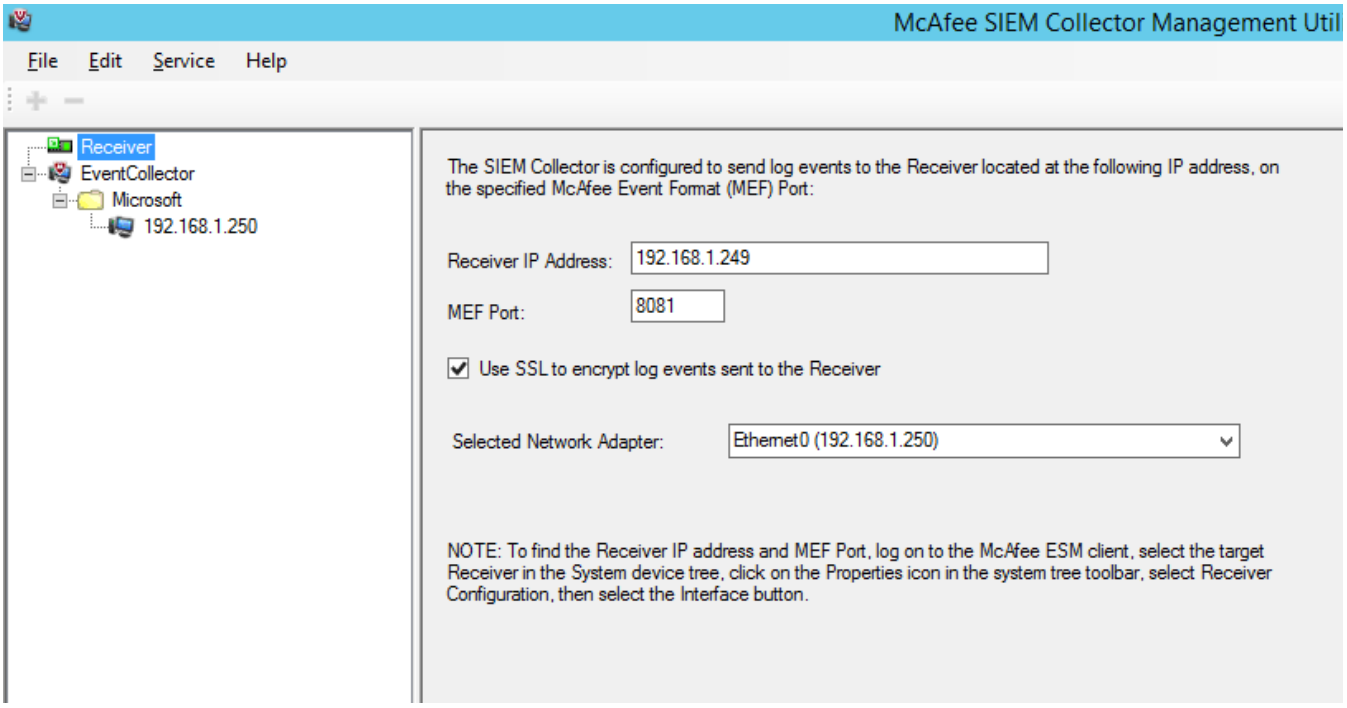
Enable the DNS logs on the Microsoft DNS Server.

1) Open the Domain Name System Microsoft Management Console (DNS MMC) snapin.
2) Click Start, Programs, Administrative Tools, and then DNS.
3) From the DNS Server, right-click the server and select Properties submenu.
4) The Properties pop-window will appear on your screen.
5) Select the Debug Logging tab and the Log packets debugging check box, respectively.
6) Ensure that the Incoming, UDP, Queries/Transfer, and Request check boxes are selected.
7) The file is located at: systemroot\System32\Dns\Dns.log.



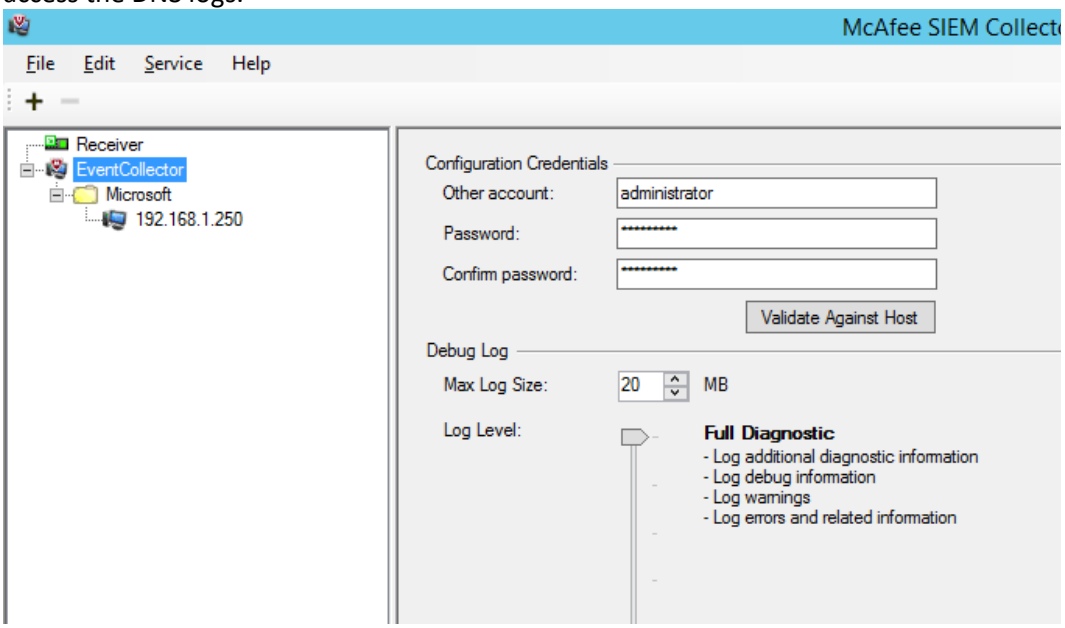
Configure the SIEM Collector to send DNS logs over to ESM

1) After the SIEM Collector is installed, launch the program.
2) Enter the Receiver IP address and ensure the port is 8081.

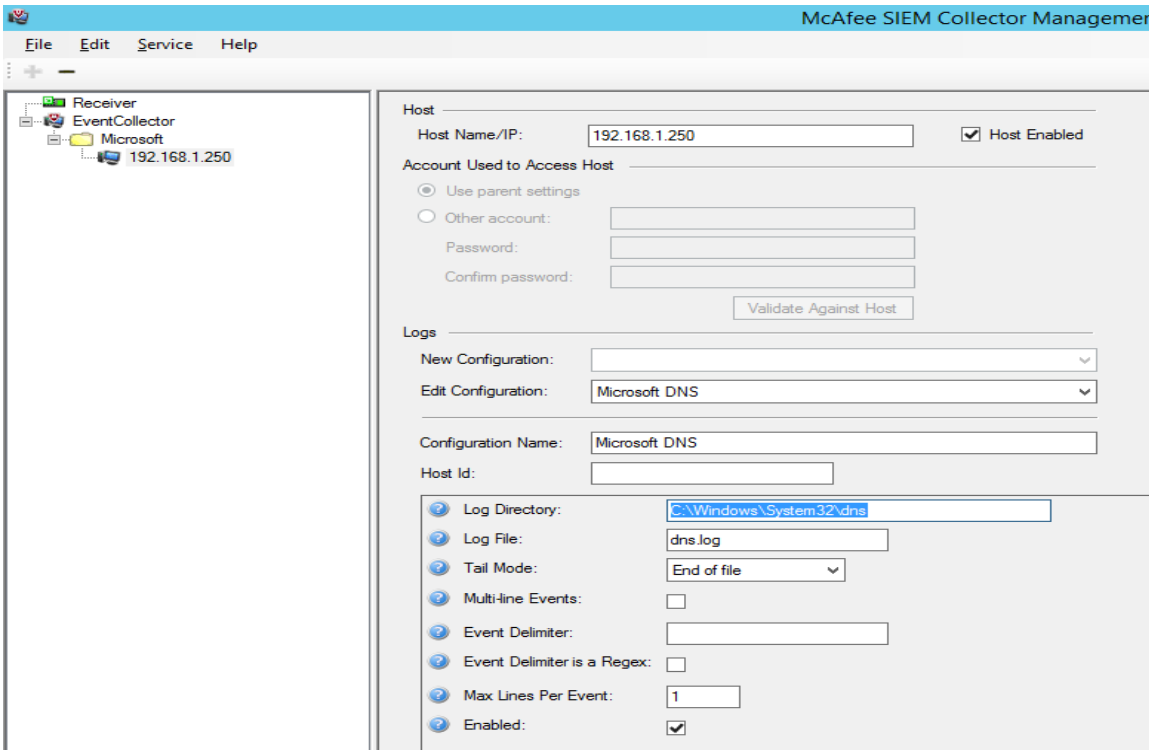


3) Under the Event Collectors, right click on it and create a new group.

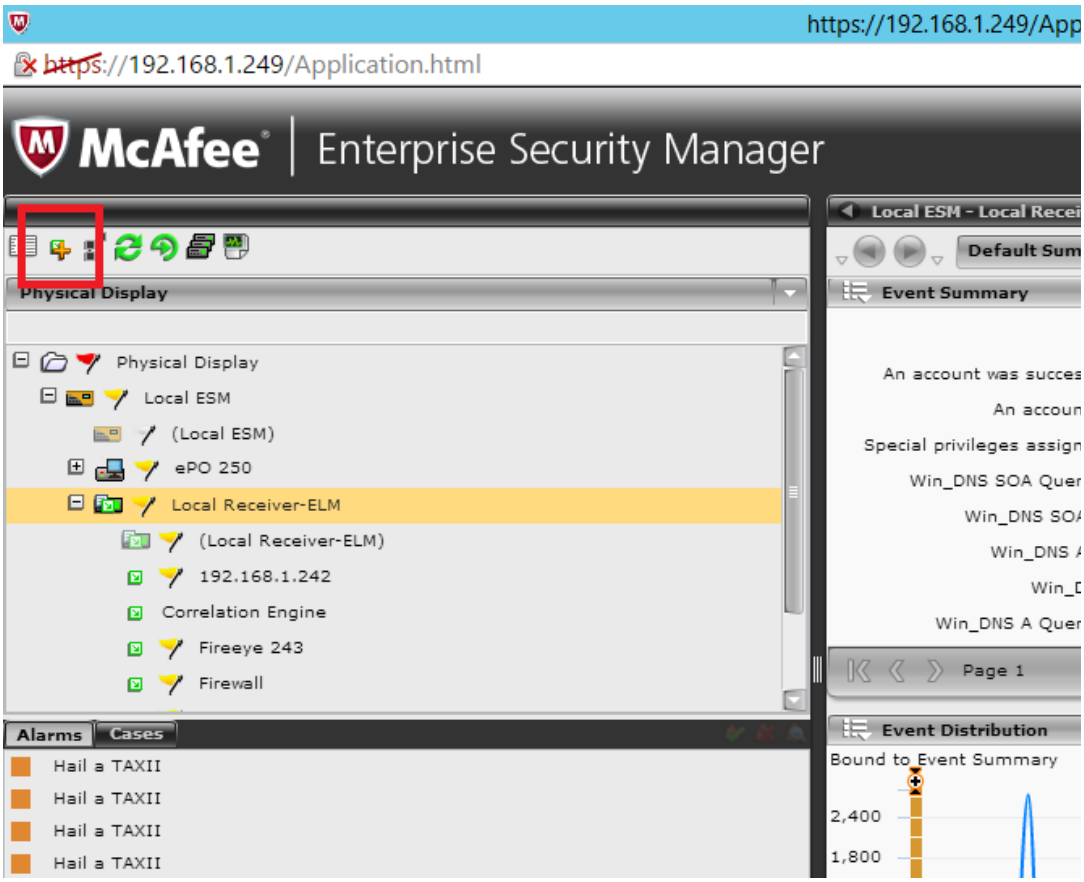
4) In the group options, enter your credentials for the Windows Server. These credentials are to access the DNS logs.



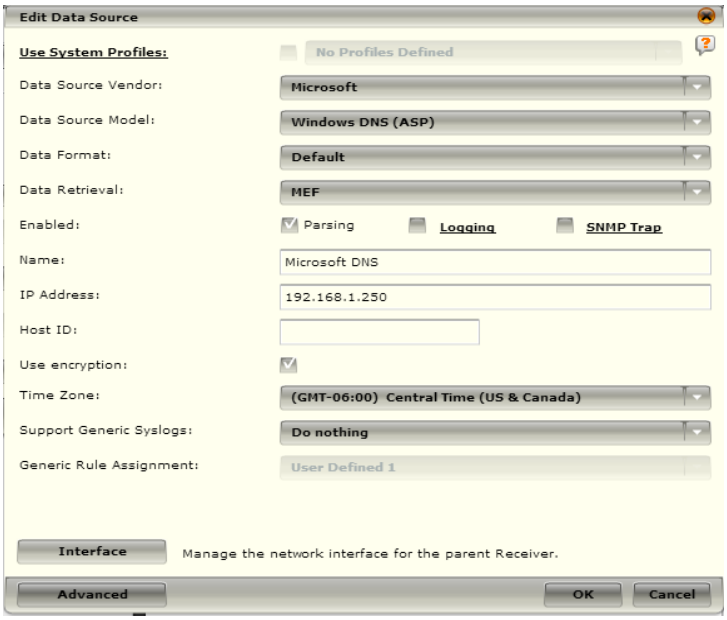
5) Right click on your group and click on Add Host. This will be the settings for your host and collector. Enter your Host Name/IP at the top.
6) Next, create and name a new configuration and enter the details for your DNS log. We're going to tail the end of the log file and send it to the McAfee ESM.
   - Log Directory: C:\Windows\System32\dns
   - Log File: dns.log
   - Tail Mode: End of file
   - Enabled: Checked



7) Log into ESM in order to setup the receiver to receive the data.
8) Select the Local Receiver.
9) Click the “Add Data Source” icon.



10) On the Data Source screen, input the below.
    - Data Source Vendor – Microsoft
    - Data Source Model – Windows DNS (ASP)
    - Data Format – Default
    - Data Retrieval – MEF
    - Enabled: Parsing/Logging/SNMP Trap – <Default>
    - Name – Name of data source
    - IP Address/Hostname – The IP address and host name associated with the data source device (IP must match that of the SIEM collector's)
    - Host ID – Host ID associated with the SIEM Collector log tail configuration if applicable
    - Support Generic Syslogs – Do nothing
    - Time Zone – Time zone of data being sent

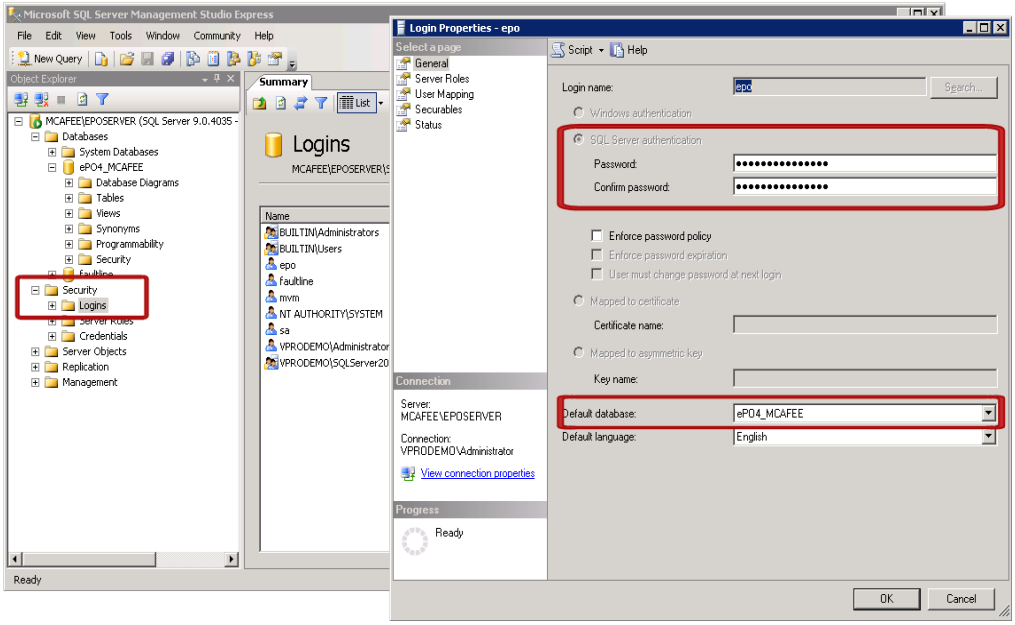


Adding HBSS (ePO) Data Source

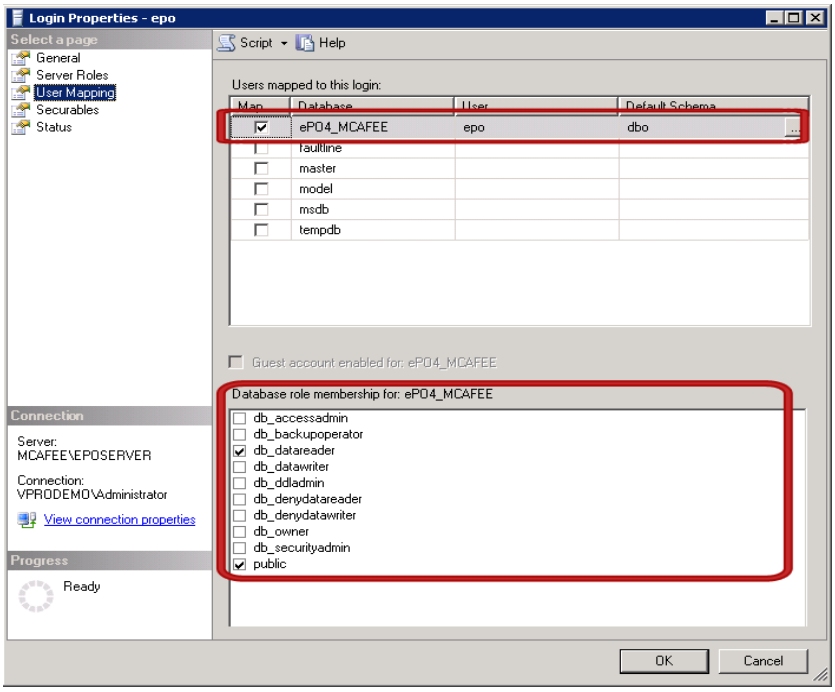
The McAfee SIEM supports event collection from ePolicy Orchestrator via a connection to the ePO SQL database. To define an ePO Data Source connection, you will require a SQL account on the ePO database server with sufficient privilege to read from the ePOEvents table.

The following outlines the configuration steps required on the ePO server.

1) Ensure that a SQL Login account is available with appropriate privilege to the McAfee ePO database. For this example, an account named 'epo' has been created using SQL authentication and a Default Database set to that of the ePO database.

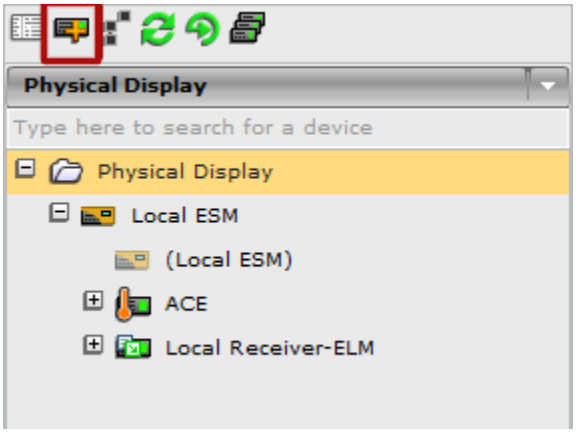


2) Configure the appropriate User Mapping, granting Public and db_datareader roles to this user.



The following outlines the configuration steps required to add the ePO Data Source to an ESM running version 9.2.0 or higher.

1. With the Physical Display selected on the System Tree, click the Add Device button from the Action Toolbar located in the upper left of the interface.



2. The Add Device Wizard window will open. From the Add Device Wizard window, select McAfee ePolicy Orchestrator (v4.6 or newer) and click Next.

   NOTE: Depending upon the appliance deployed in the POC, some of the device options may not be available as indicated by the device type being greyed out. This is expected in POC installations deployed using an All-in-One combo appliance.

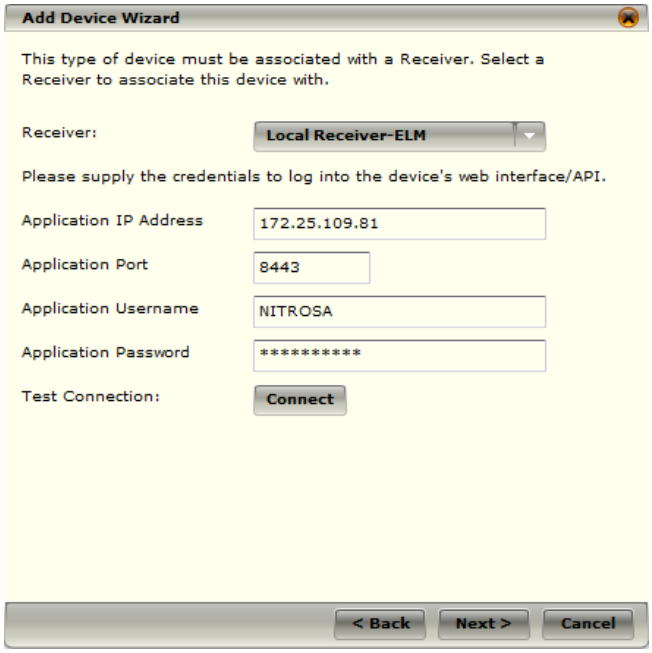
3. Enter a Name for this ePO Data Source.

NOTE: Each application installed in ePO (VSE, HIPS, etc.) will be added to the ePO data source as children using this name as a prefix. Example: McAfee ePO_VirusScan, McAfee ePO_Application and Change Control, etc. To prevent these child data source names from becoming truncated, use a short descriptive name for the parent ePO data source.

4. Click Next.

   The ePO data source requires information relating to both the ePO Application Server and the ePO Database Server. In some ePO deployments this may be the same host however appropriate credentials must be supplied individually for each. Application credentials are used for the purposes of connecting to the ePO server to apply policy tags while database credentials are used by the SIEM to retrieve events for analysis, correlation and reporting.

   The Wizard will prompt you for both the Application details as well as the Database details on separate windows starting with the ePO Application information.
5. Select the Receiver on which this ePO data source will reside.
6. Enter the IP Address of the ePO Application Server.
7. Enter the appropriate Application Port (default is 8443).
8. Enter the Application Username.
   NOTE: The ePO user provided must have Group Admin privileges assigned within ePO.
9. Enter the Password assigned to this ePO user.



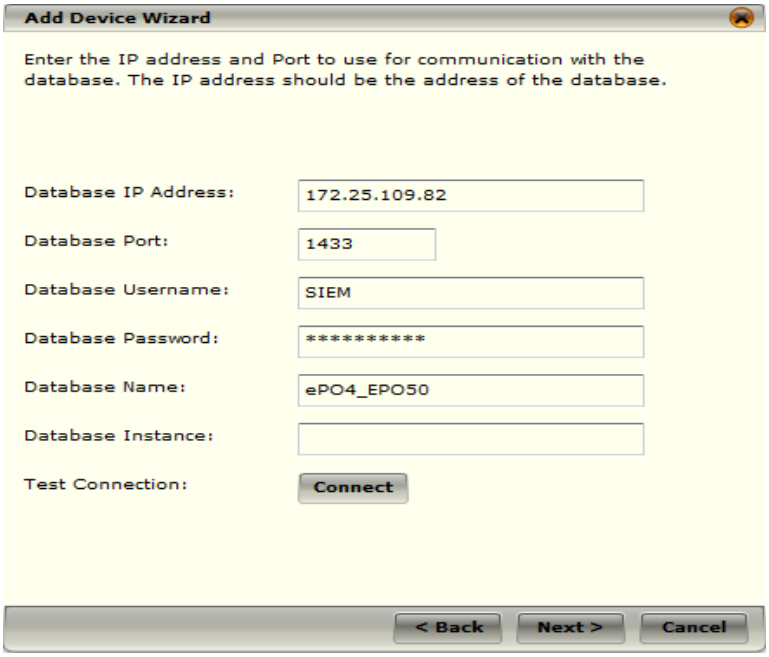
10. Click the Connect button to test the connection to the ePO application. If the connection is completed successfully, a confirmation dialog box will open. Click Close. If the connection test is unsuccessful, verify the ePO user credentials and privileges.
11. Click Next.

    The Wizard now prompts you for the ePO Database details.

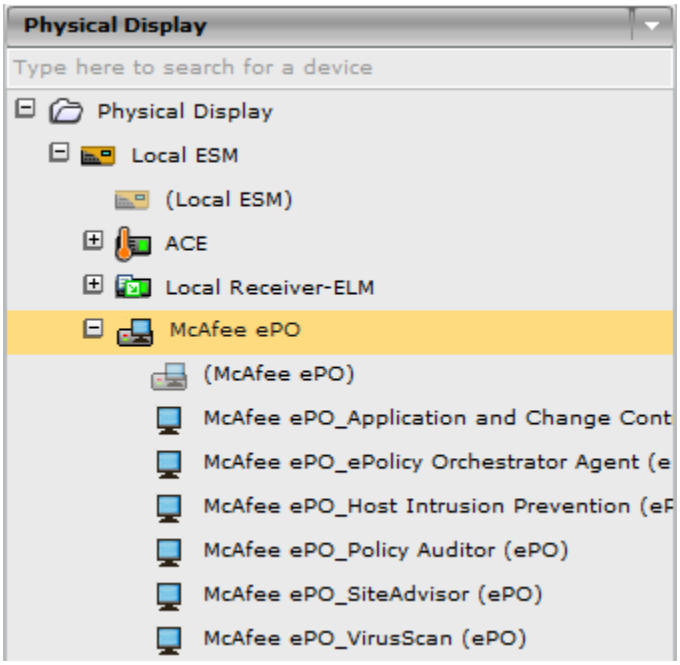
12. Enter the IP Address of the ePO Database Server.
13. Enter the User ID of the SQL Login Account created earlier.
14. Enter the Password assigned to the SQL Login Account.
15. Enter the appropriate SQL Communication Port (default is 1433).
16. Enter the ePO Database Name.

    NOTE: If the ePO Database Name contains a hyphen, the value entered MUST be surrounded by square brackets. Example: [ePO4_MCAFEE-123]

17. If multiple SQL instances are present on this database server, enter the unique Database Instance associated with ePO.



18. Click the Connect button to test the connection to the ePO database. If the connection is completed successfully, a confirmation dialog box will open. Click Close. If the connection test is unsuccessful, verify the SQL credentials and privileges.
19. Click Next.
20. A dialog box will open regarding the use of McAfee Risk Advisor data within the SIEM. The McAfee SIEM can utilize Risk Advisor asset reputation scoring as a component of a Risk Correlation policy. If Risk Advisor is present in the ePO installation AND if the Advanced Correlation Engine is being deployed with the SIEM, click Yes.
21. Once complete, the Add Device Wizard will present a status window indicating that the ePO data source was successfully added and configured.
22. Click Finish.
23. Expand the new ePO Data Source in the Device Tree to confirm the connection to the ePolicy Orchestrator host and to identify the McAfee products that were found to be installed.



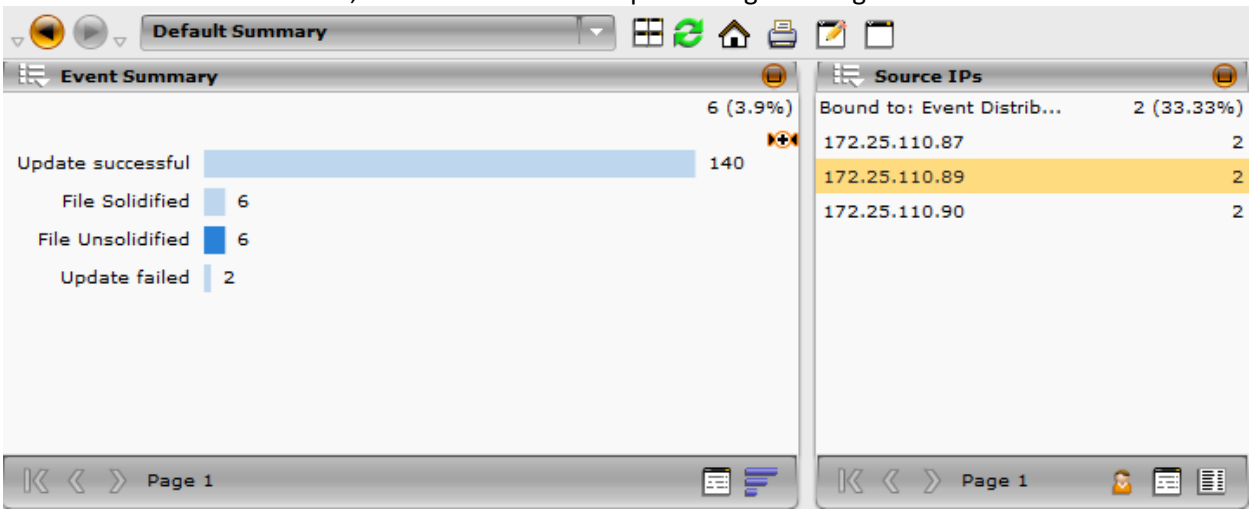
Configuring Advanced ePO Integration

The McAfee SIEM supports the ability to launch ePO directly from the SIEM interface to view endpoint details as defined within ePolicy Orchestrator. This advanced integration assumes that you have properly configured the Local Network settings in the Asset Manager (Directions are found in the guide in Configuration section with the Server Setup section. Please ensure you have followed the steps to configure Local Network before continuing.

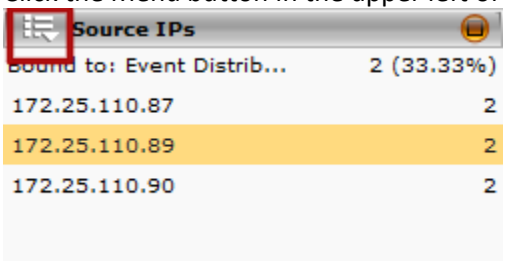
Testing Advanced ePO Integration

Once the McAfee SIEM has been configured with at least one ePO data source and the Local Network value has been defined within the Network Discovery section of the Asset Manager, the SIEM will allow the operator to launch the ePO interface from within the Security Management platform to view asset details specific to a given endpoint.

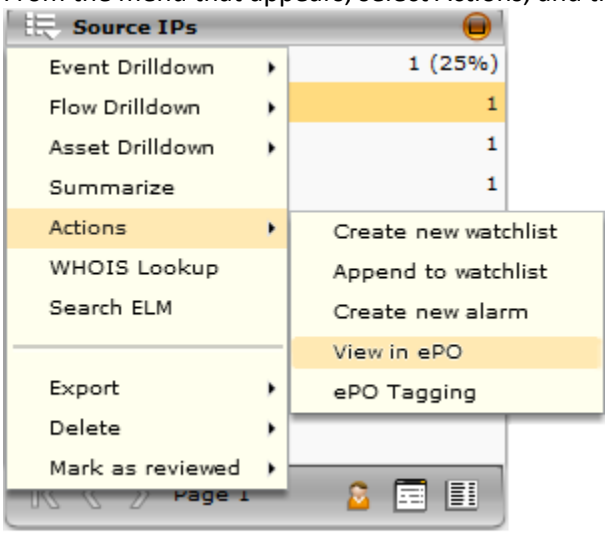
1) From the SIEM user interface, select an IP address representing a managed asset within ePO.



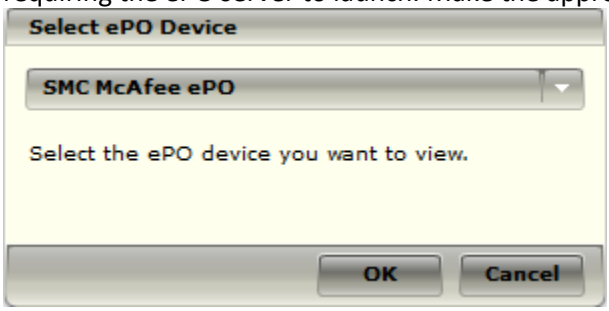
2) Click the Menu button in the upper left of the Source IP Address component.



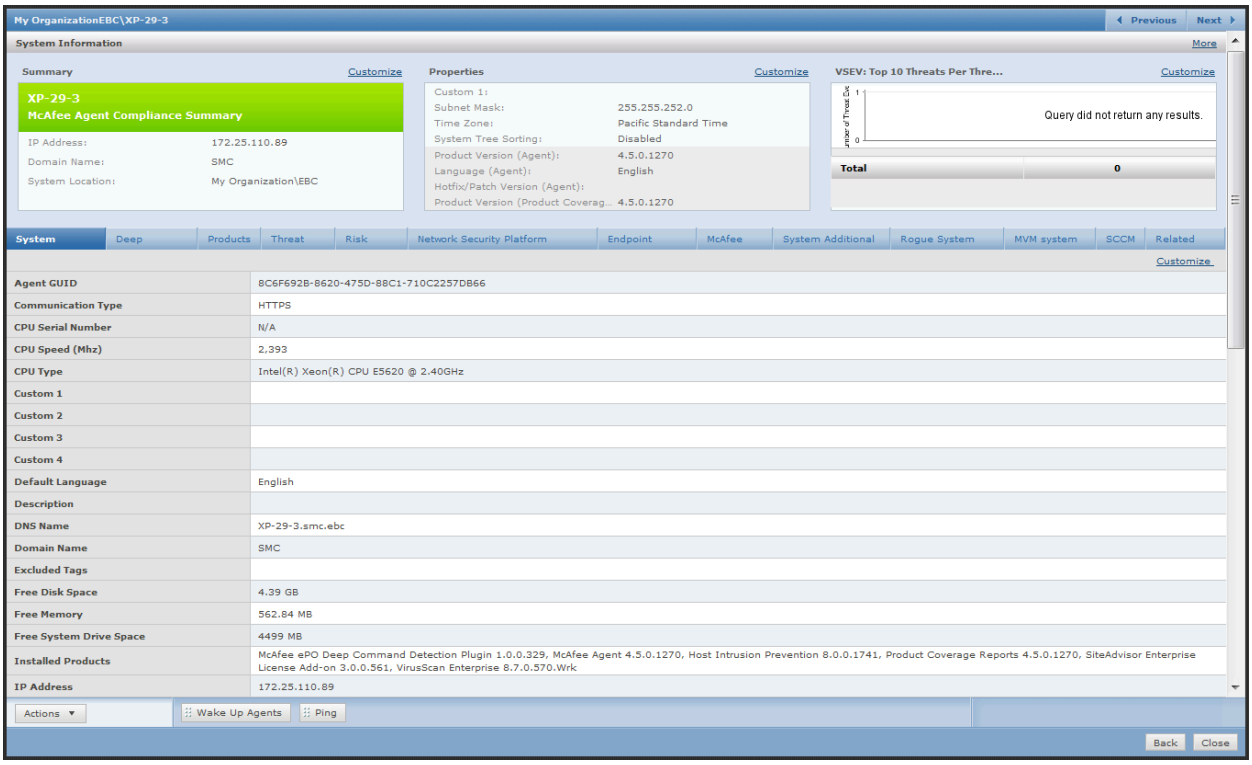
3) From the menu that appears, select Actions, and then View in ePO.



4) If multiple ePO servers are defined in the McAfee SIEM, an additional dialog box will open requiring the ePO server to launch. Make the appropriate selection and press OK.



5) The ePO interface will open in a new browser window requiring authentication. Enter the appropriate ePO credentials to log into the ePolicy Orchestrator interface.
6) Once authenticated, the ePO asset information window will open displaying the information related to the endpoint selected in the McAfee SIEM.



Adding Bro IDS Data Source

By default, there is one Bro parser built-in to ESM and it is for DNS logs. We can build custom parsers for the other Bro logs, which are addressed in the Advanced Syslog Parser section of this document. Without a parser for the other logs, the data can be received but ESM will not know what to do with it. We can also drop the logs we don't have a parser from.

To add a data source to receive Bro logs:

1) On Security Onion, open /etc/syslog-ng/syslog-ng.conf.
2) Search for "destination d_elsa" and right before it, copy and paste the below. The only thing that needs to change is the IP address to that of your ESM.

   Note: Only the logs that have a parser on ESM will be read correctly. So if there is no parser, just omit the specific line. This will help with the efficiency of ESM.

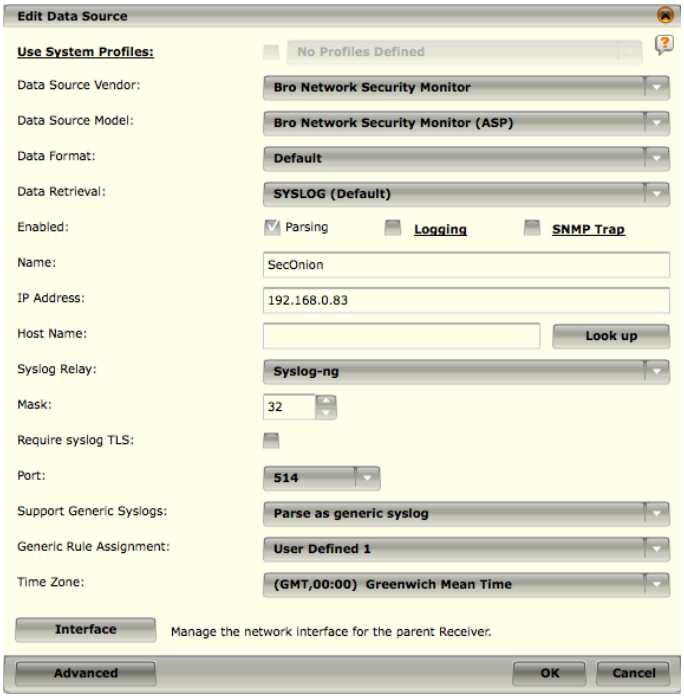
   Note: Out of the box, ESM comes with the DNS parser already. I have built a parser for the conn log, which is included in this document in the Advanced Syslog Parser section.

```
destination d_siem { syslog("123.456.789.012" transport("udp")); };

log {
      source(s_bro_conn);
      source(s_bro_http);
      source(s_bro_dns);
      source(s_bro_weird);
```

```
        source(s_bro_tunnels);
        source(s_bro_syslog);
        source(s_bro_ftp);
        source(s_bro_files);
        source(s_bro_dhcp);
        source(s_bro_notice);
        source(s_bro_smtp);
        source(s_bro_smtp_entities);
        source(s_bro_ssl);
        source(s_bro_irc);
        source(s_bro_software);
        source(s_bro_ssh);
        source(s_bro_intel);
        source(s_bro_x509);
        source(s_bro_snmp);
        source(s_bro_radius);
        source(s_bro_mysql);
        source(s_bro_kerberos);
        source(s_bro_rdp);
        source(s_bro_pe);
        source(s_bro_sip);
        log { destination(d_siem); };
};
```

3) Save the conf file and restart syslog-ng (service syslog-ng restart).
4) On ESM, highlight the Receiver and click on the plus sign to add a data source. Fill in the information as shown below (except for the IP address and Name).



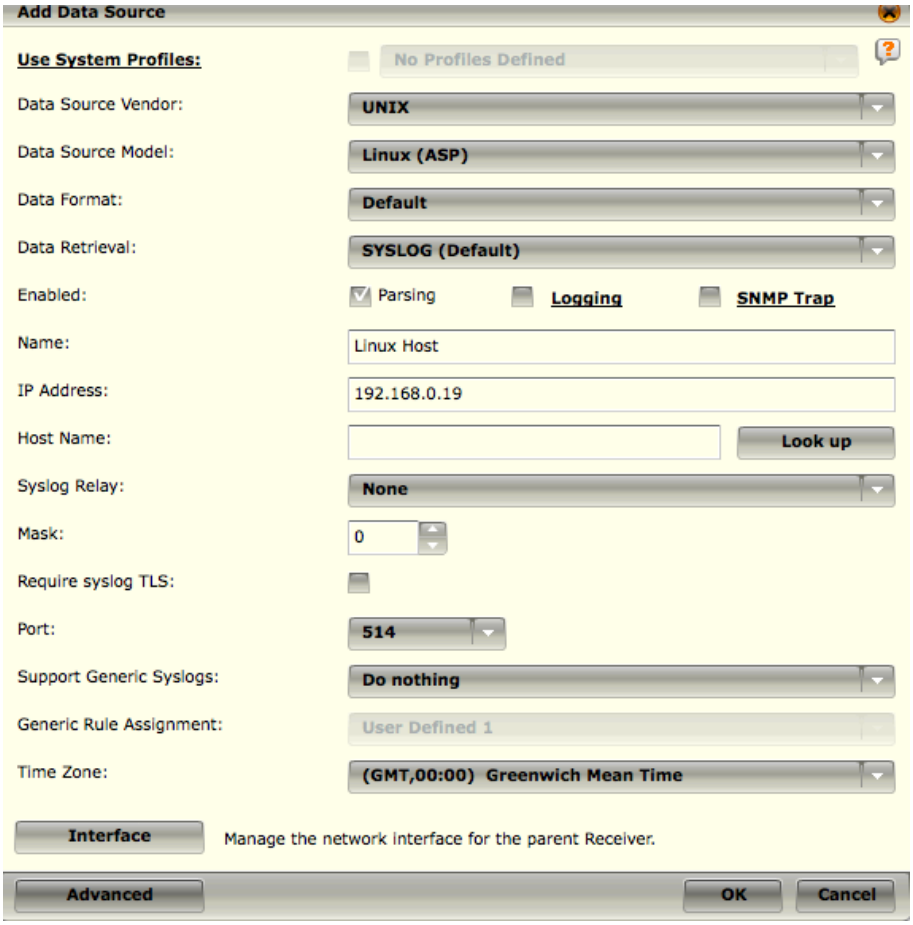
5) Click OK.
6) Click Yes twice.
7) Click OK.
8) Click Close.
9) The newly created data source will now be visible.

Adding Linux or Other SIEM Data Sources

For the most part, *nix systems have a syslog server capability. With that said, all that is needed on the ESM side is to create a data source to enable the receiving of that information.

1) Click on the Receiver in the window on the far left.
2) Click to open the Receiver properties.
3) Configuration should be similar to the below image, aside from the IP and Name.

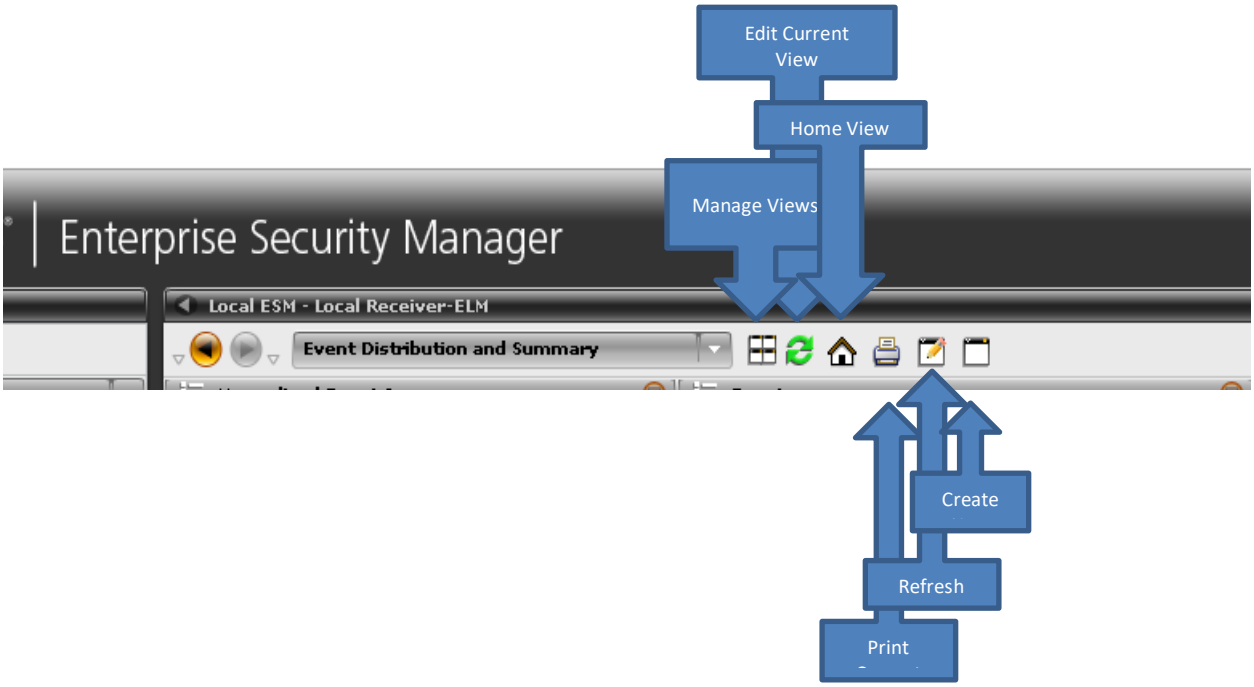
> Note: If the events being received are tagged with a different time zone, please use that. ESM will then normalize to the time zone of the server.
>
> Note: If using receiving from Splunk, Security Onion, or anything that uses Syslog-ng, change to relay to suitable option.



4) Click OK.
5) Click Yes twice.
6) Click OK.
7) Click Close.
8) The newly created data source will now be visible.

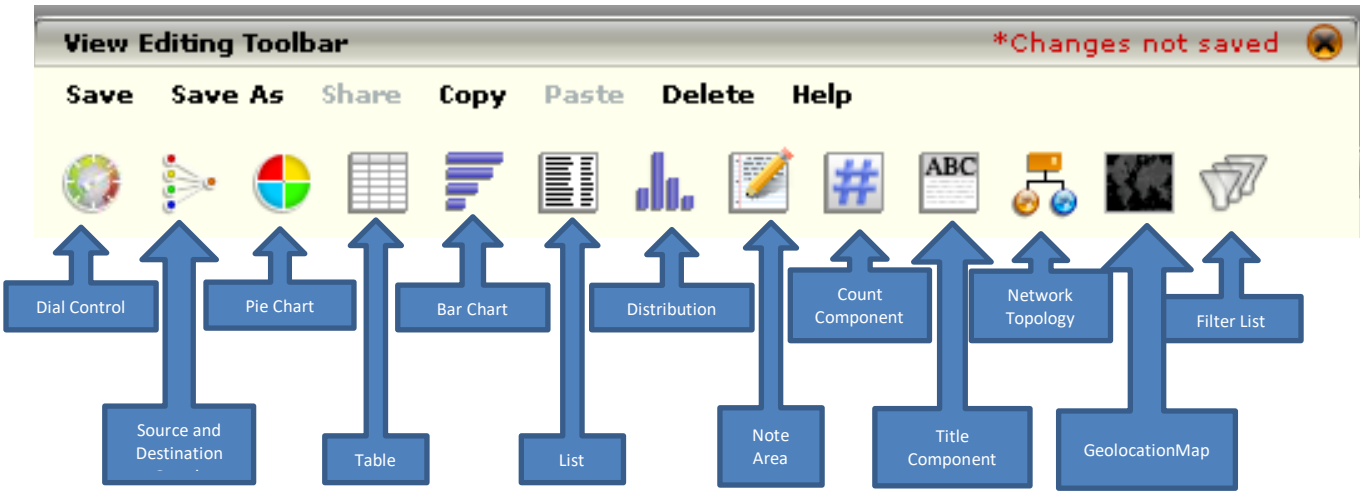
Dashboard

On the Dashboard toolbar, there are six available options, which are shown listed below.



To create a dashboard, do the following:

1) Click on the "Create New View" icon as noted above.
2) You will then be presented with a blank dashboard and an editing toolbar as shown below.



Each one of the available options on the editing toolbar serves a specific purpose. I will attempt to highlight a few things about each but for a more in-depth understanding of dashboards as a whole, I recommend viewing the video located at https://community.mcafee.com/videos/1447.

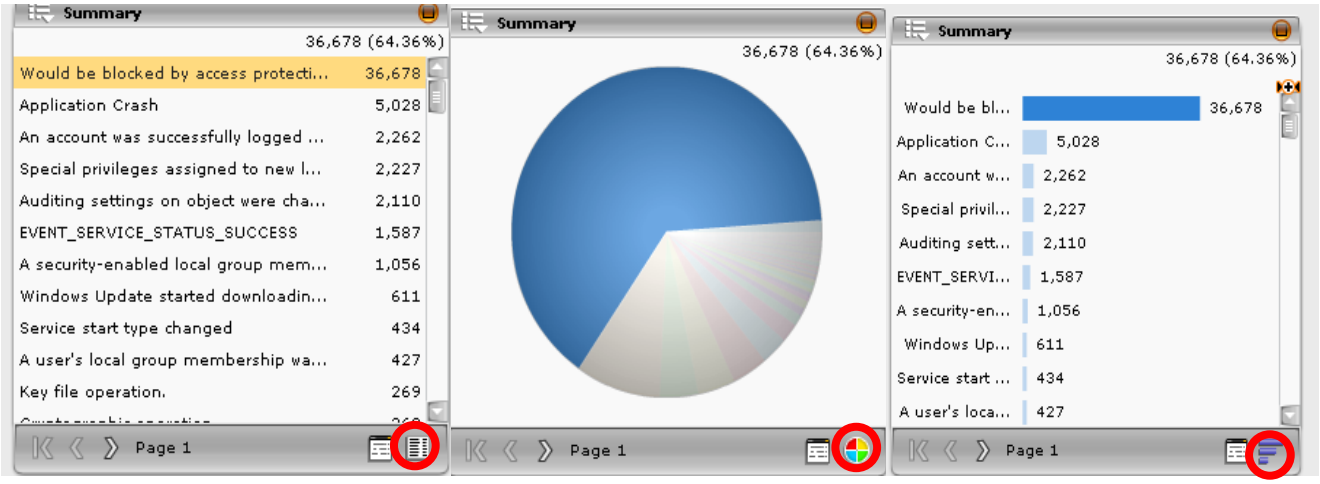
All the edit toolbar options support some variation of the below options.

- Event Queries
- Flow Queries
- Case Management
- Asset and Vulnerability
- Risks Status

Pie chart, bar chart, and list

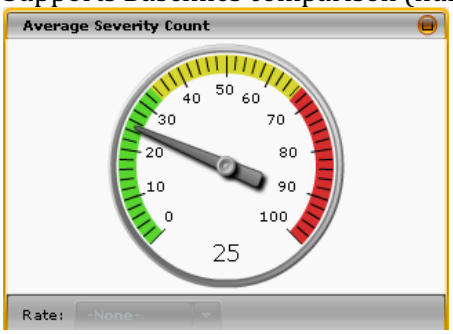
- Can filter and sort based on specific criteria
- Supports Baselines comparison (number of events at a specific time compare to now)
- You can drilldown into events and output data to another view
- You can alter between the views using the icon in the bottom right corner as shown below

Table **Pie** **Bar**



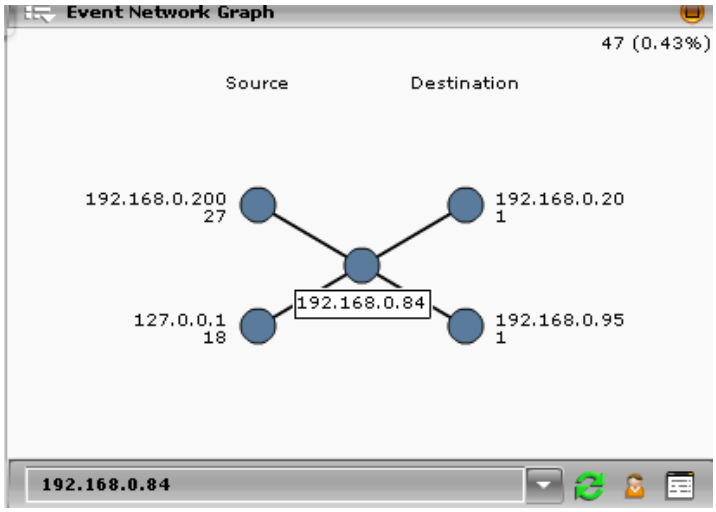
Dial Control

- Can filter and sort based on specific criteria
- Supports Baselines comparison (number of events at a specific time compare to now)



Source and Destination Graph

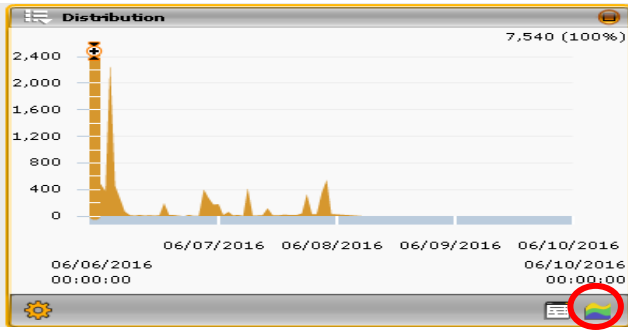
- Can filter and sort based on specific criteria
- Shows Flow data
- You can drilldown into events and output data to another view
- Supports Baselines comparison (number of events at a specific time compare to now)



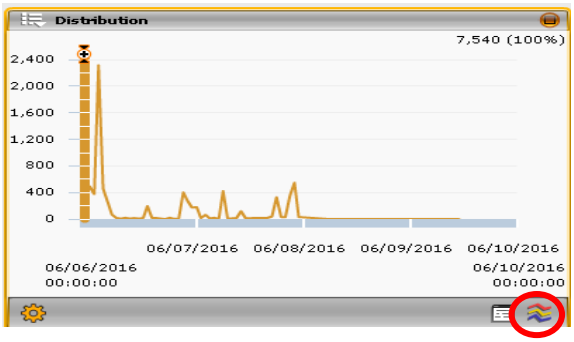
Distribution

- Supports Baselines comparison (number of events at a specific time compare to now)
- Can filter based on specific criteria
- You can drilldown into events and output data to another view
- Multiple available views that can be changed by clicking the icon in the red circle below

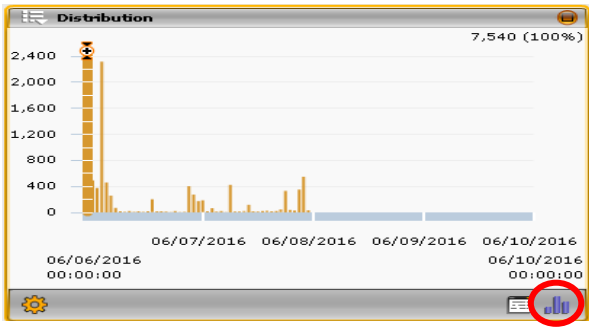
Column



Lines

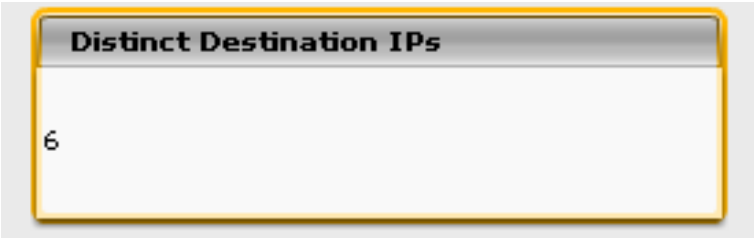


Area



Counts

- Gives you a total count based upon specified criteria
- Can filter and sort based on specific criteria



Title Component

- Use to provide a title on a dashboard. This is different from the dashboard name given when creating the dashboard. This could be used to provide more context and information regarding the dashboard. The Notes widget is very similar to this widget except Notes actually has the word “Notes” on the widget.

Note Area

- Use to provide notes on a dashboard.

Geolocation Map

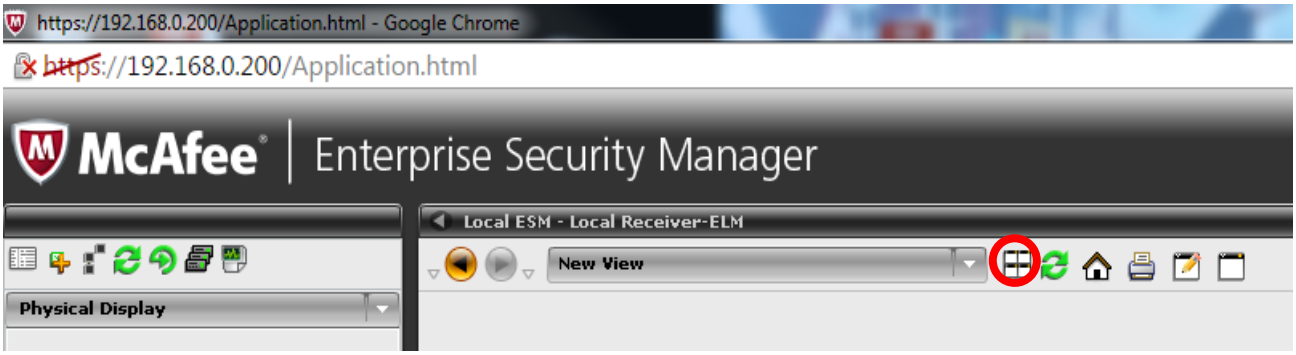
- Shows a map based on the geographic locations of specified traffic.

Event Network Topology

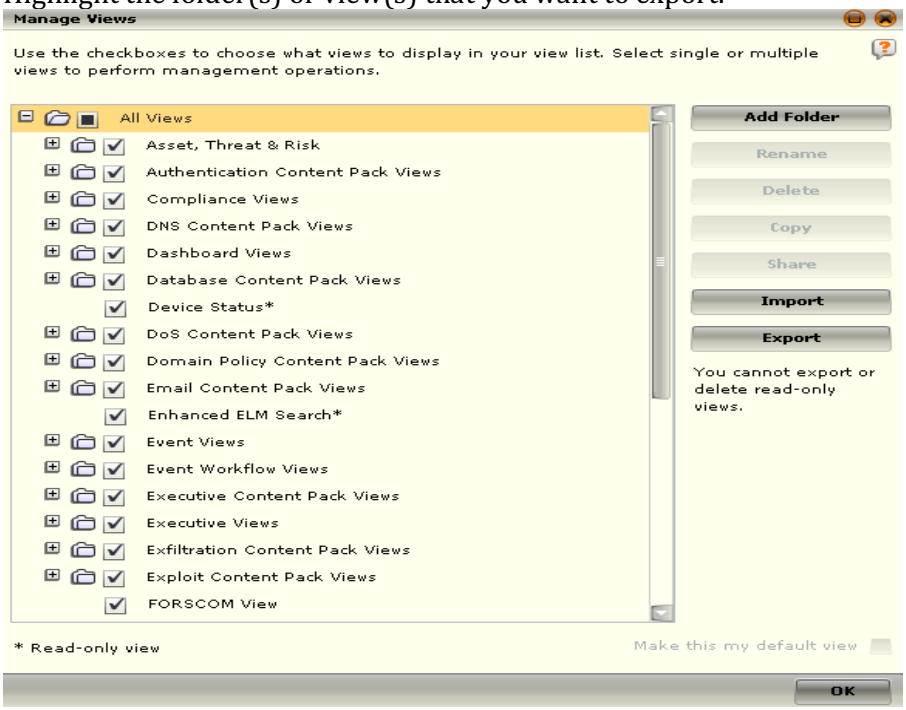
- Relies on Network Discovery
- Assists with basic network management
- You can drilldown into events and output data to another view

Export Dashboard Views

1) Click on Manage Views from the dashboard toolbar as shown below.



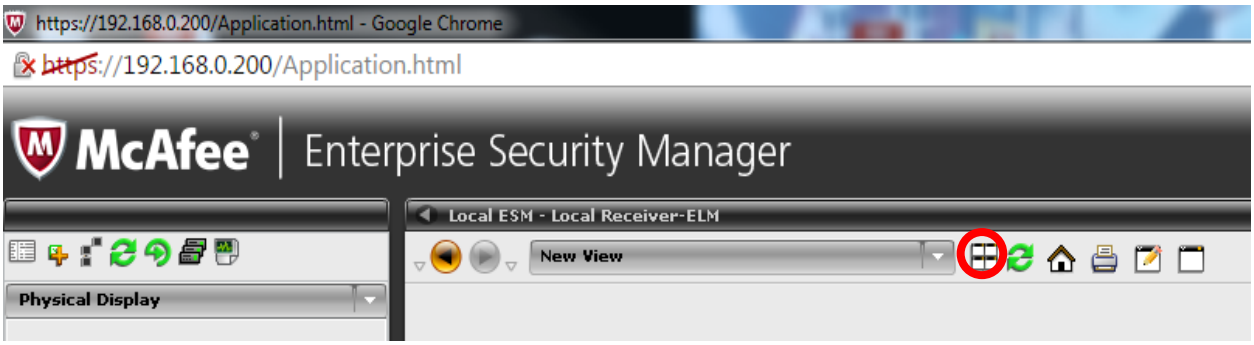
2) Highlight the folder(s) or view(s) that you want to export.



3) Click Export.
4) Click export again.
5) Click Yes to download when prompted.
6) Give the file a name and select a location.
7) Click Close when it is complete.

Import Dashboard Views

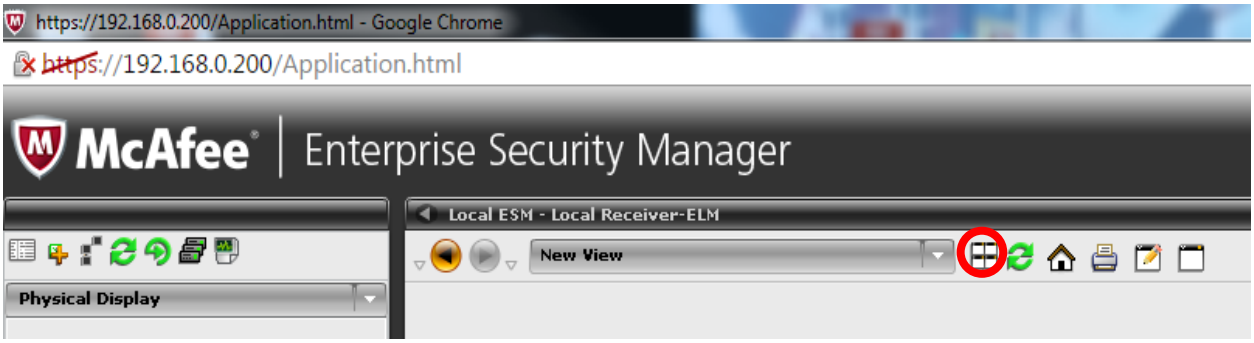
1) Click on Manage Views from the dashboard toolbar as shown below.



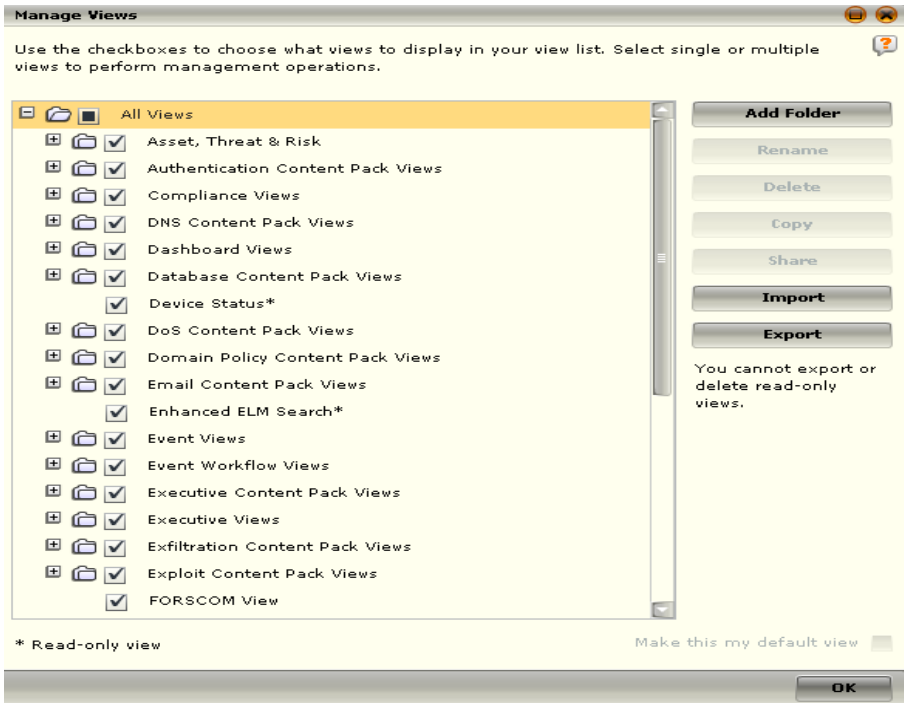
2) Click Import.
3) Click on "Choose File".
4) Navigate to the file and click Open.
5) Click Upload.
6) Click OK twice
7) The newly imported dashboard view will be visible.
8) Click OK to close the screen.

Hiding Dashboard Views

1) Click on Manage Views from the dashboard toolbar as shown below.



2) When presented with the below window, uncheck any view that you don't want to be visible. To unhide a view, just place a checkmark next to it again.



Watchlists

A watchlist is a grouping of specific types of information that can be used as filters or as an alarm condition so you are notified when they occur in an event. Watchlists, by themselves, are simply lists, and don't do anything so it is imperative that they are connected to an alarm or filter. For example:

- A watchlist can be used as a filter for a view or report. When you select a filter, you will see a tab labeled "Watchlist". If you select this tab, you will see the watchlists you have defined that are relevant to the data element you're filtering. For example, if you are filtering a source IP address, you will see the "IP Address" watchlists.
- A watchlist can be used as a trigger for an alarm. When properly configured, your alarm will trigger any time the ESM receives an event with a data field that matches the watchlist you've selected. For example, you might create a list of critical user names, and then set an alarm to fire any time an event occurs for one of these users.
- A watchlist can be used as a component in a correlation rule. This gives you a great deal of flexibility in identifying specific conditions a rule triggers, or does not trigger. As an example, you might have a watchlist that keeps track of your Vulnerability Scanner IP addresses. You might have a correlation rule that identifies systems that are scanning your network, but incorporate exceptions into the rule by including a condition that ignores scans coming from IPs that are on the watchlist.

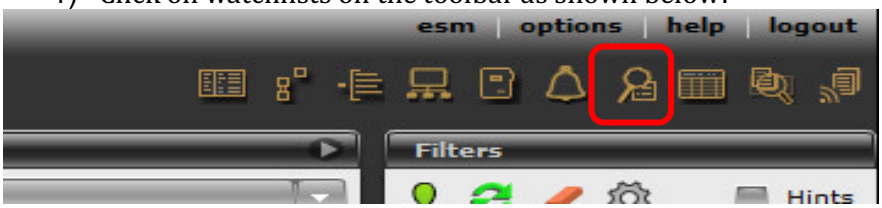
To get a better understanding of watchlists, Source IP addresses is one example of how these can be used.

Example 1: The “Suspicious Source IPs” watchlist could be a ‘bad’ watchlist
- This watchlist could be attached to an Alarm or could be used in a filter.

Example 2: The "Scanner Source IP" watchlist could be a 'good' watchlist for the Nessus scanner
- This watchlist could be attached to an Alarm where a detected Port Scan event AND it is not a match on this Scanner Source IP Watchlist triggers an Alarm.

Create a Watchlist

1) Click on watchlists on the toolbar as shown below:

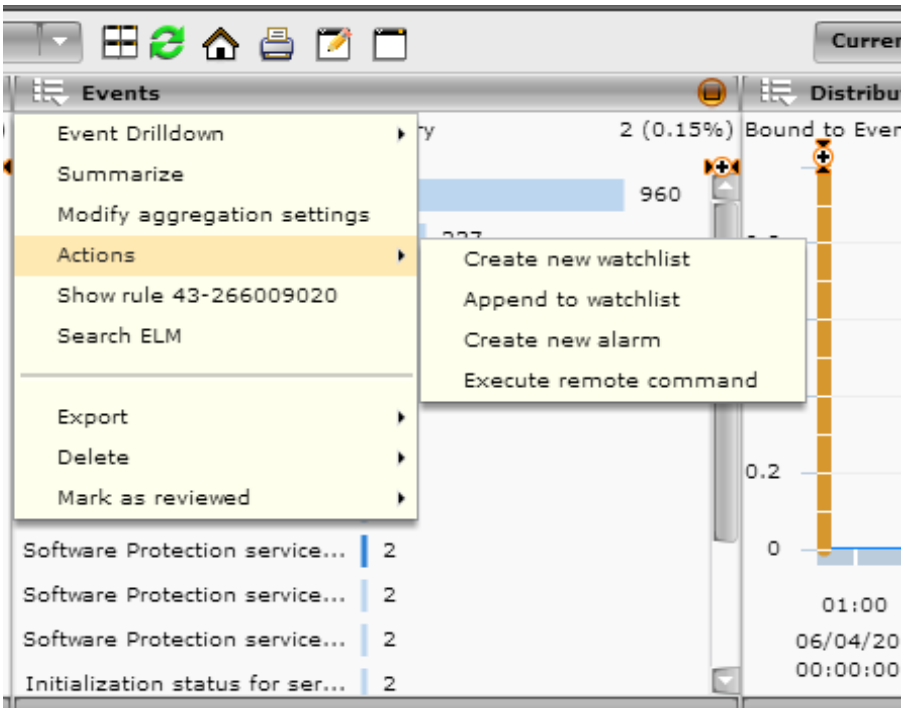


2) Click Add.
3) Give the list a name and if you want it to expire, set the parameters.
4) Click the Value tab.
5) Select the suitable type. Below are a few good choices to use:
   - DNS Name
   - File Hash
   - File Path
   - File Size
   - Filename
   - IP Address
   - Any of the ones starting with Destination or Source.
6) Once the type is chosen, input the Values.
7) Click Finish.

Note: It is recommended to create an alarm and reference this watchlist in order for something to actually happen. More information and linking the two can be found in the Alarm section of this guide.

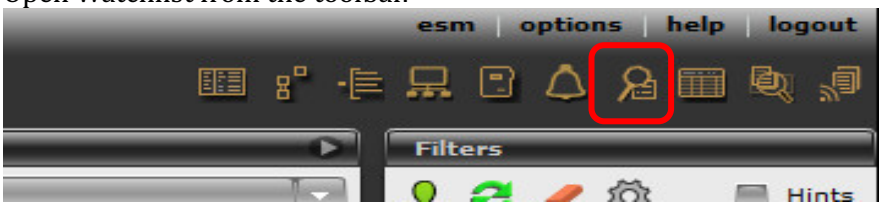
Create Watchlists from Events

1) Click on the event you want to add.
2) Click Event > Actions > Create New Watchlist.



Import a Watchlist

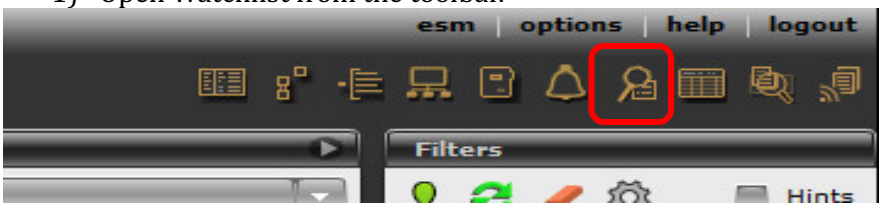
1) Open Watchlist from the toolbar.



2) Click Import.
3) Click Browse and navigate to the .xml file.
4) Click Open.
5) Click Upload.
6) The watchlist will now be present in the window.

Export a Watchlist

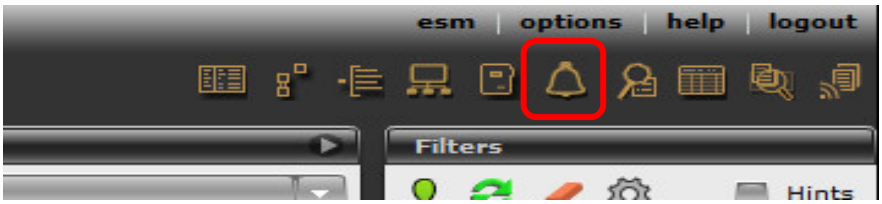
1) Open Watchlist from the toolbar.



2) Highlight the list(s) that you want to export.
3) Click Export.
4) Click Yes.

Note: Depending on the browser, you may have to select a download location.

Alarms



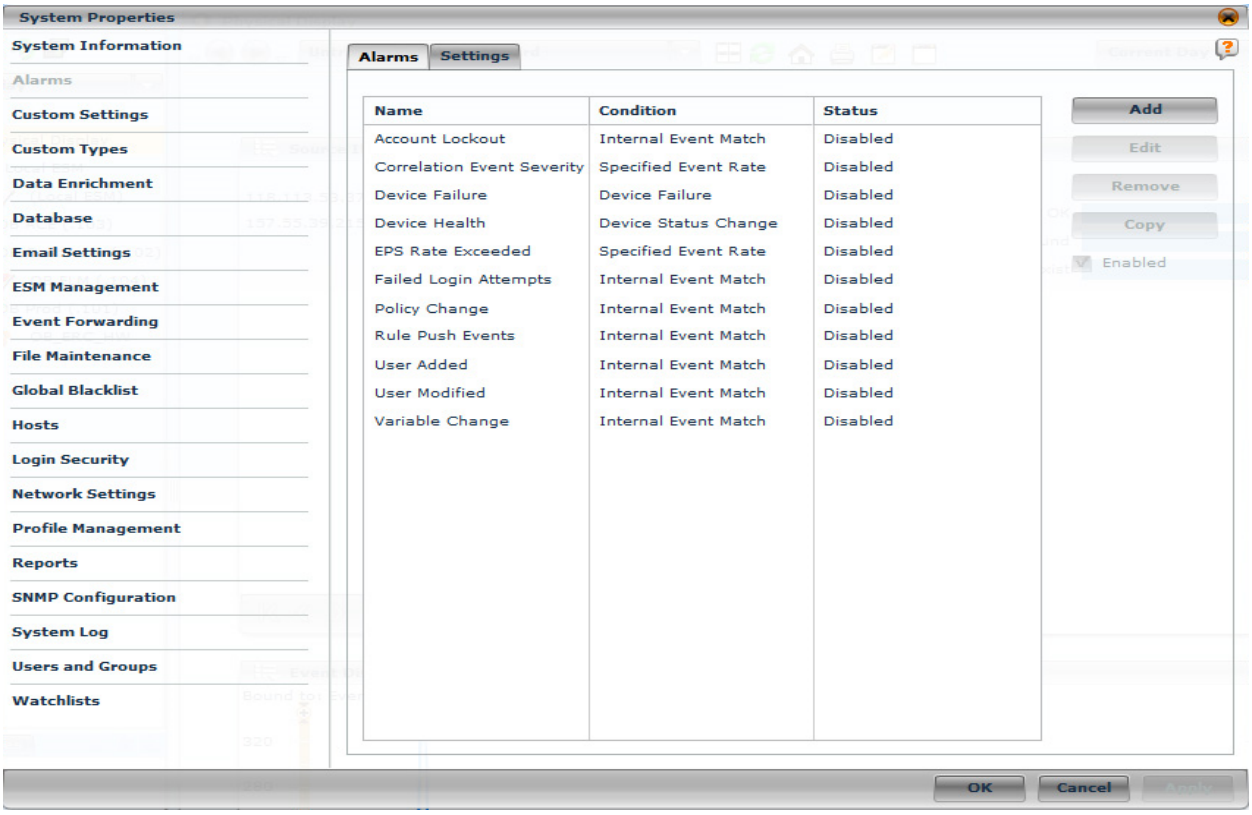
Alarms are used by the SIEM to drive actions in response to incoming events. An important part of having a sustainable, operational SIEM is having a set of alarms that provide proactive notifications of the most critical incidents for defenders. In most missions, it's not practical to have an incident responder watching a dashboard on a monitor 24x7. With a proper set of alarms, the ESM provides critical continuous monitoring functionality.

Enabling pre-built alarms

McAfee ESM comes with a minimal set of pre-built alarms to provide notifications of important events related to the ESM itself (such as device failures, unusually high event rates, user modifications, etc.) These alarms can be viewed in the Alarm Manager (System Properties > Alarms). They are disabled by default; as a starting point for any mission, it is recommended to review the canned alarms and enable alarms that represent a handful of critical events.

To enable pre-built alarms:

1) Open the Alarm Manager (System Properties > Alarms). Default alarms can be seen below.



2) Select the alarms you would like to enable. You may shift-click and control-click to multi-select.
3) Click the Enabled checkbox to enable the alarms of your choice, and then OK to save your changes.

Create alarms for events critical to your environment.

In your investigations, over time you will discover repeated patterns of behavior that represent incidents that merit real time alerting or other actions. Often there will be specific correlation rules (canned or custom) that you will use to identify these incidents.

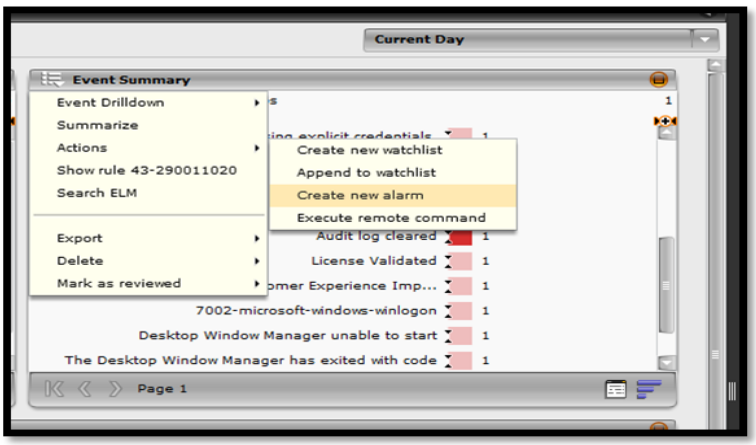
Create an Alarm from an Event

There will be times where an event will occur that you will want to setup as an alarm so you are notified of it the next time it happens. To do so, do the following:

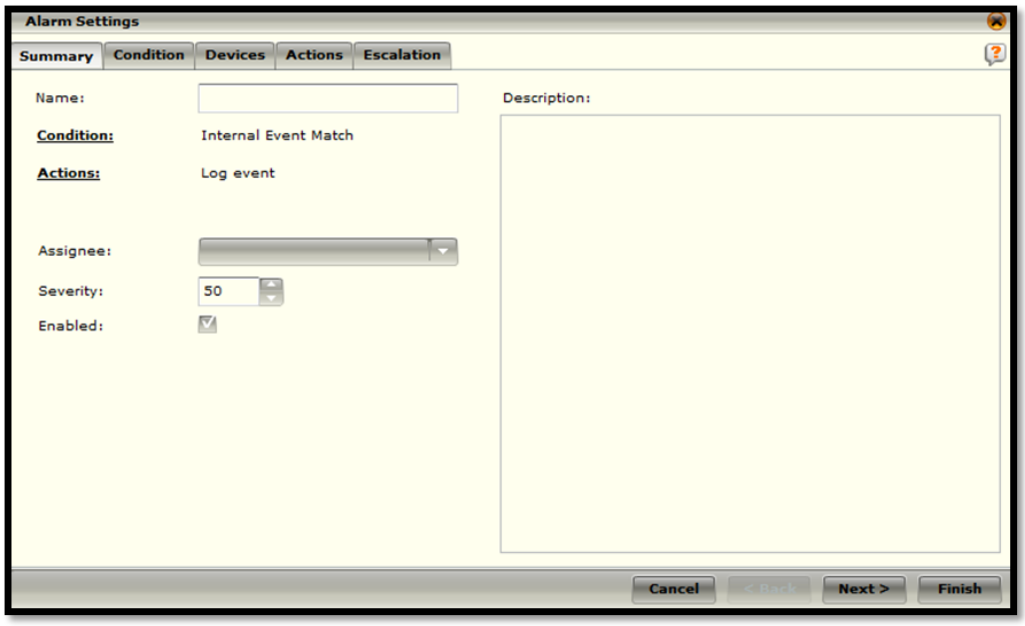
1) In the console click on the event you want to create an alarm for. In this example, we'll click on "Audit log cleared".

2) Then pull down the menu at the top left corner of the pane where the event is displayed.

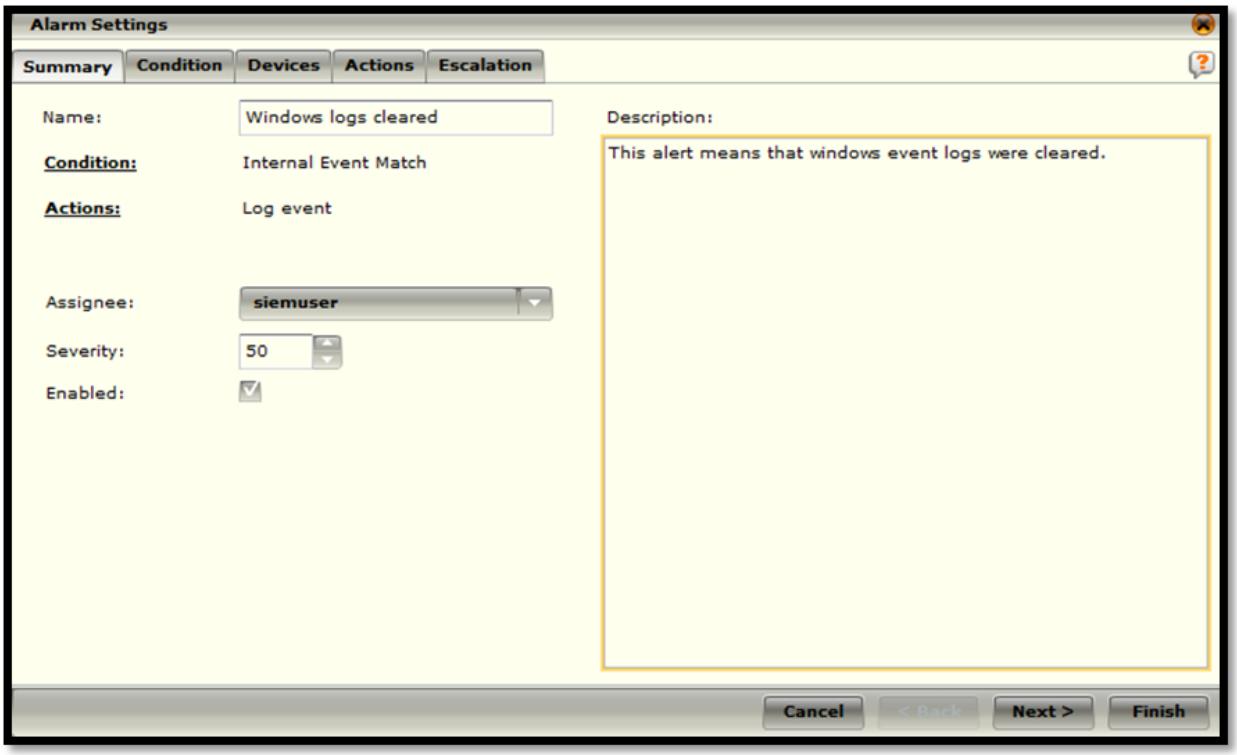
3) Select “Create New Alarm”.



4) The Alarm settings window opens.



5) Give this new alarm a name, a description and assign it to a user.

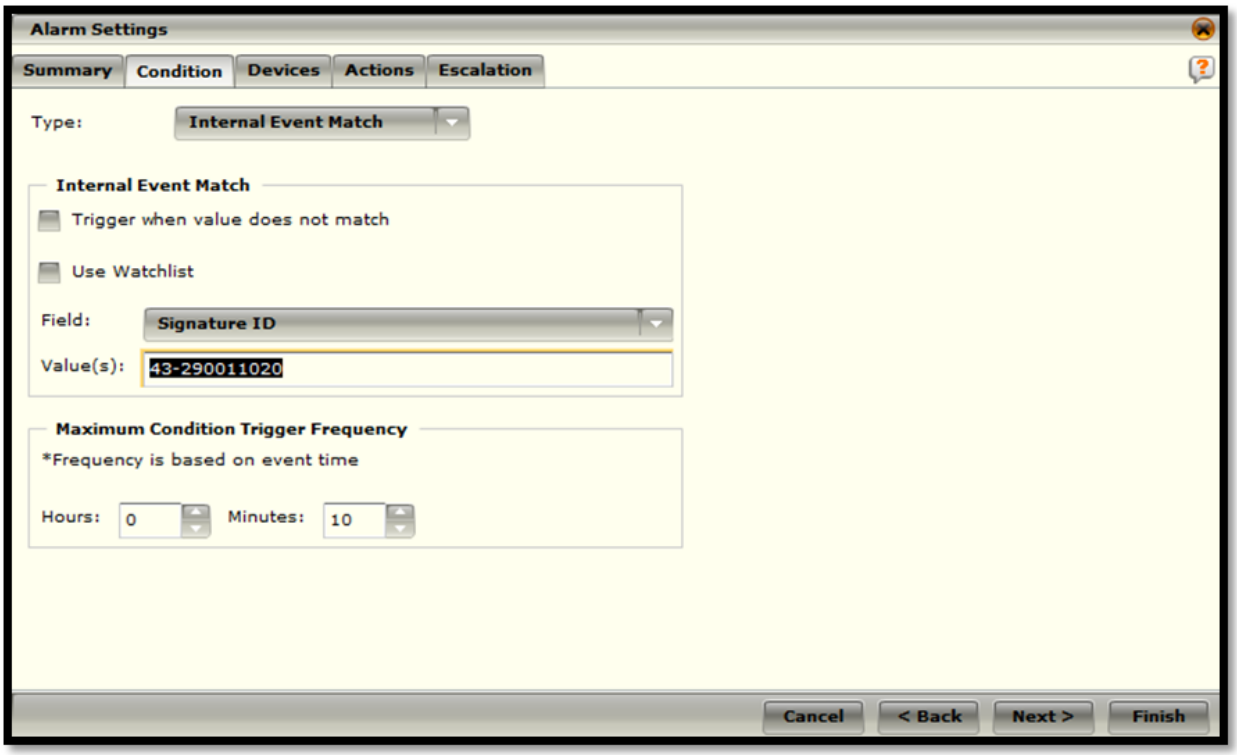


6) Click on the Condition tab to define what fields need to match for the alarm to trigger.

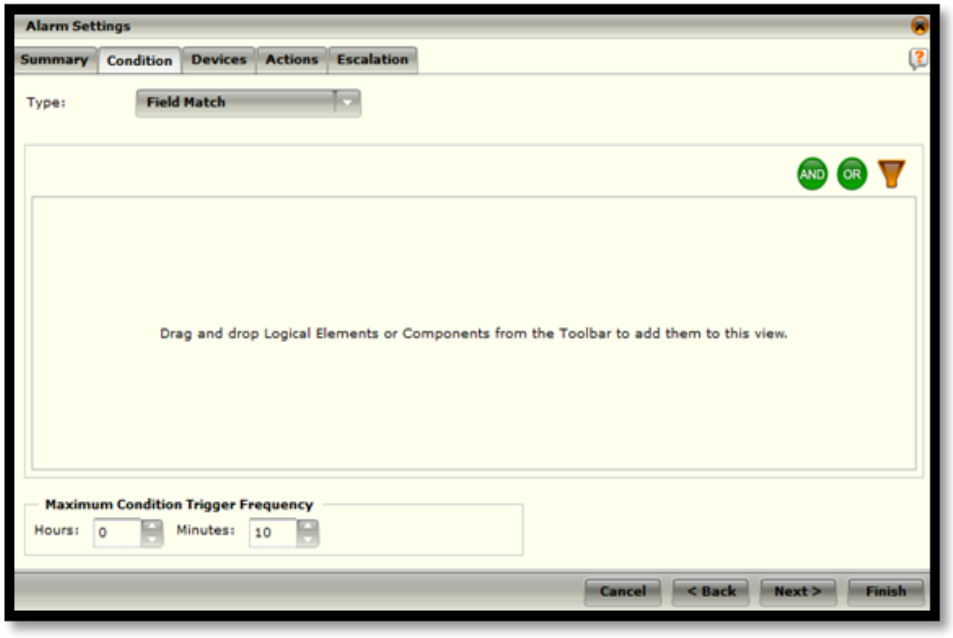
Note: We see the Signature ID that is associated with the event that we want to be alerted on. Since the signature ID is a quick and sure way to identify this event, we will use its

signature ID. I recommend that you copy the signature ID from this field, so we can use it in the next step.

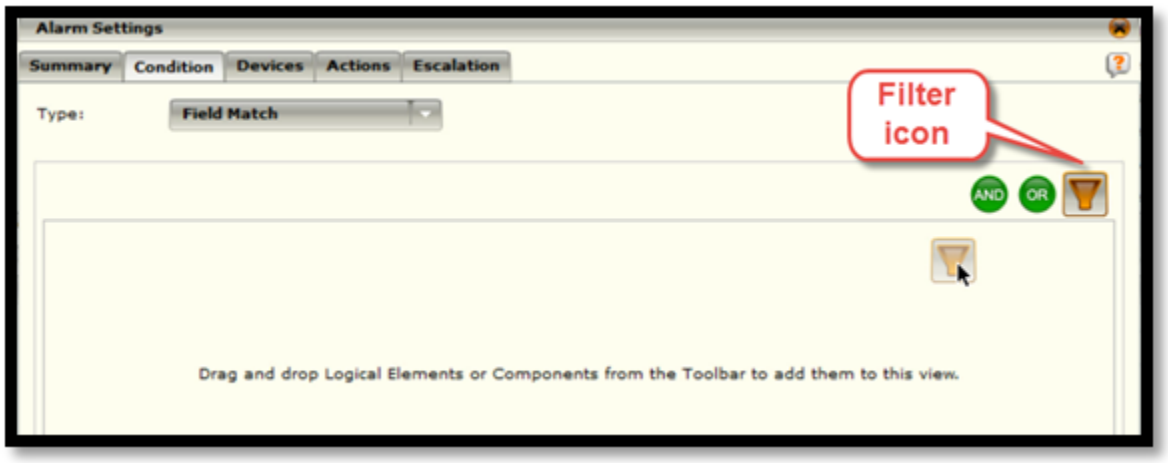
Note: This signature ID applies to Windows Security logs being cleared. Windows Application and System logs being cleared use their own signature ID. For a list of Signature IDs, look in the "Signature ID" section of this document.



7) Select "Field Match" as our type.



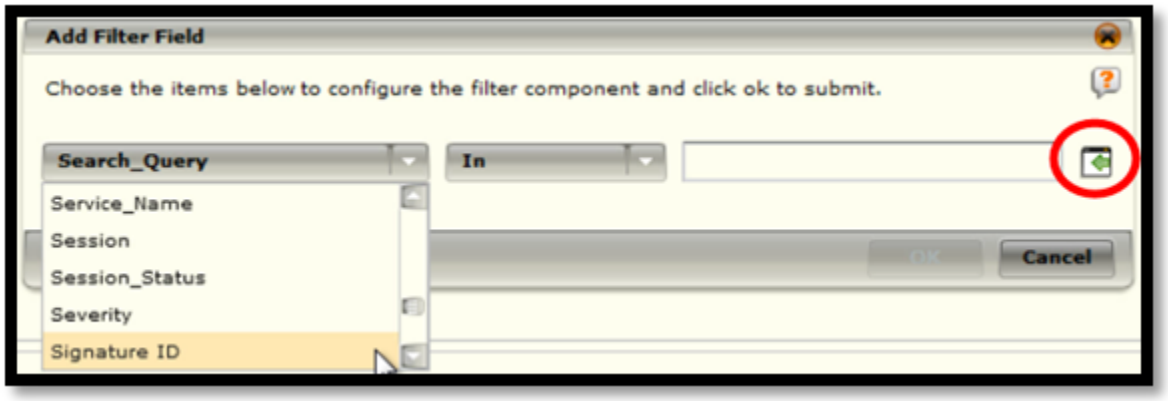
8) Drag and drop the filter icon into the view.



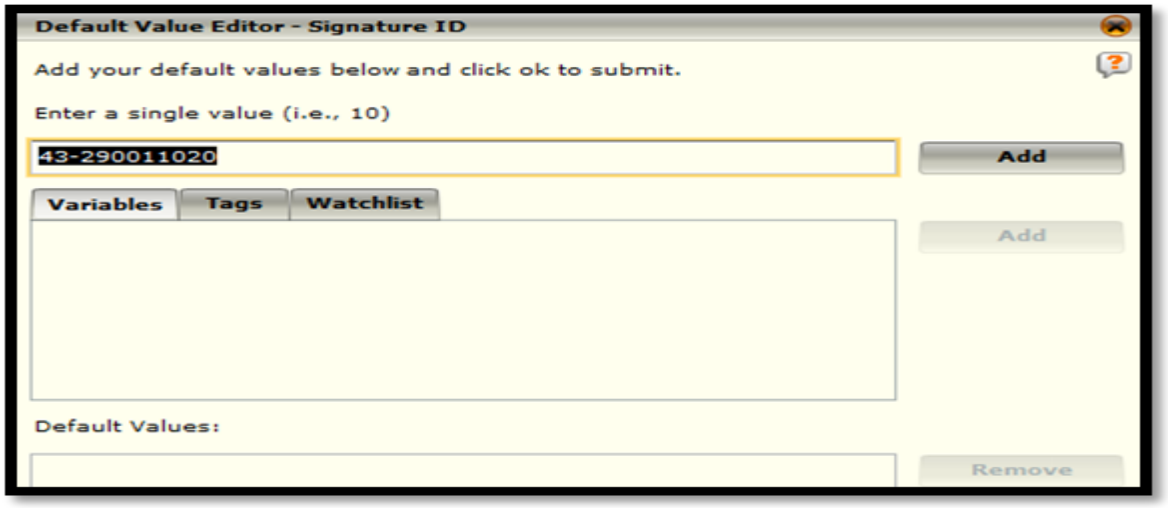
9) The add filter field window opens.

10) Select Signature ID.

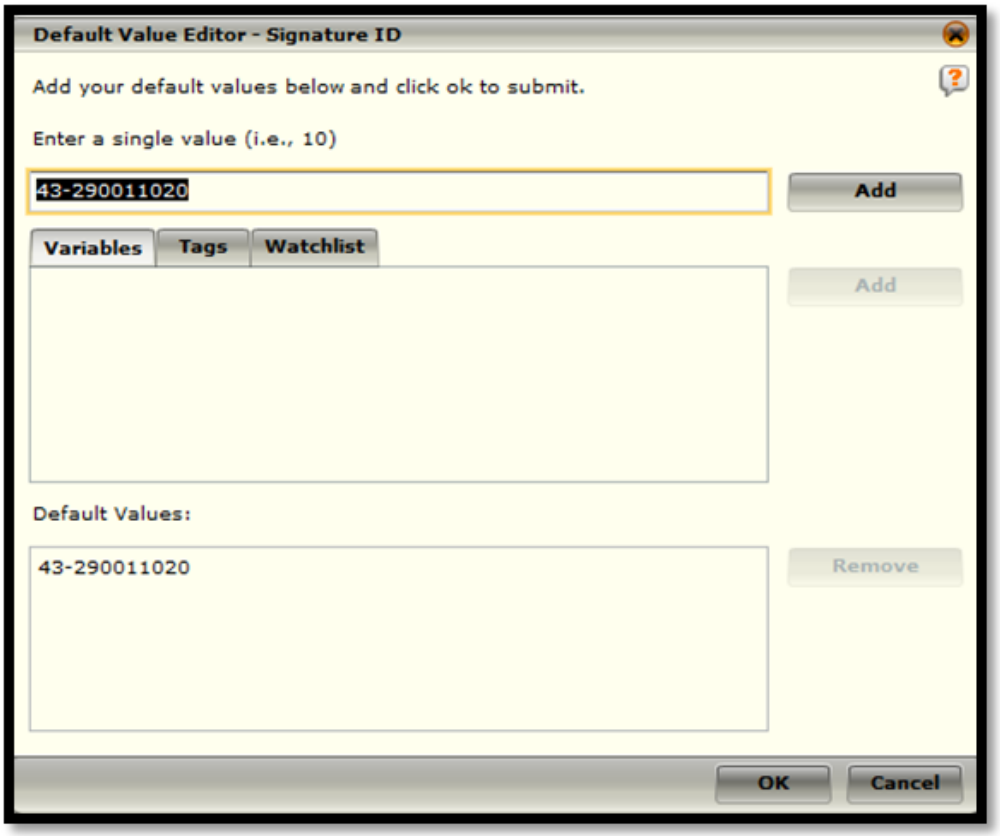
11) Click on the green arrow on the right side of the window.



12) The default value editor opens. Paste the signature ID that copied earlier on.

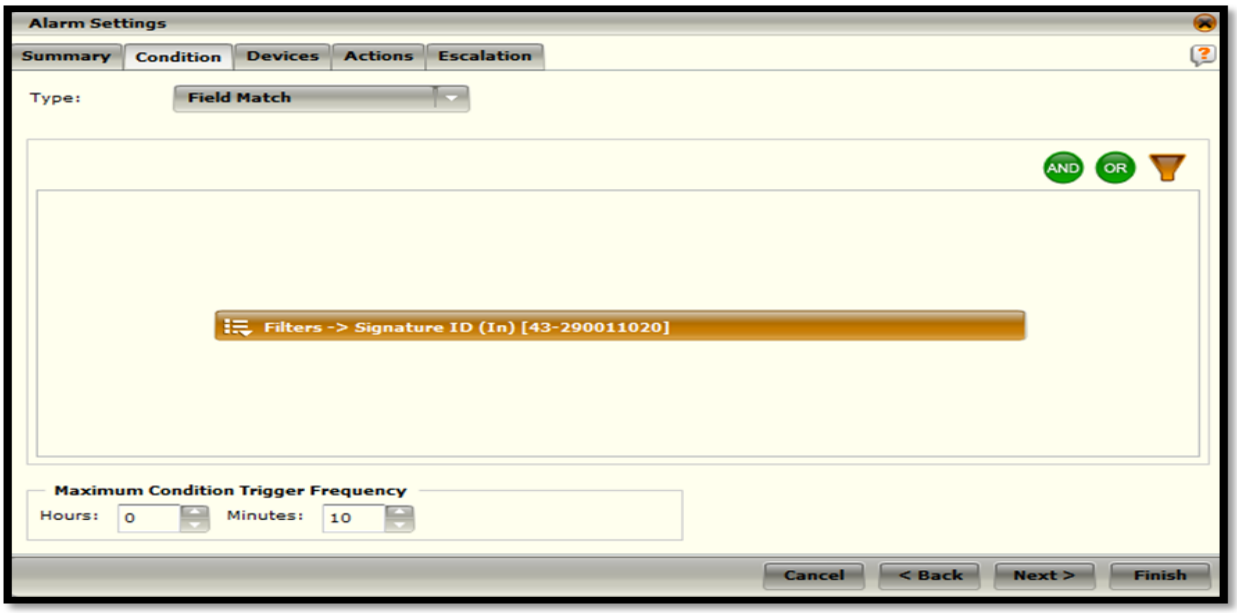


13) Click Add. The copied signature ID appears in the default value pane.

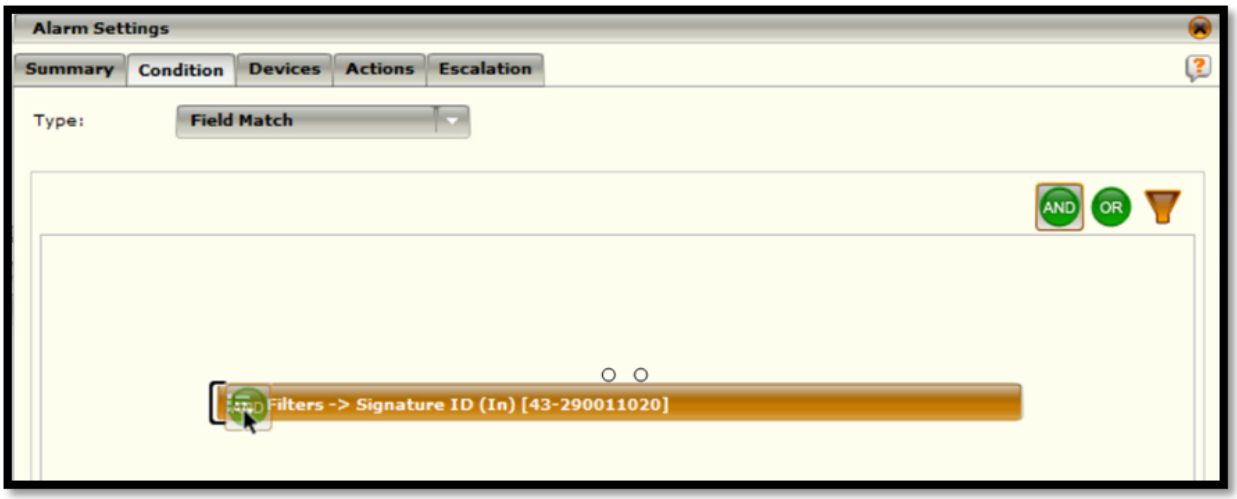


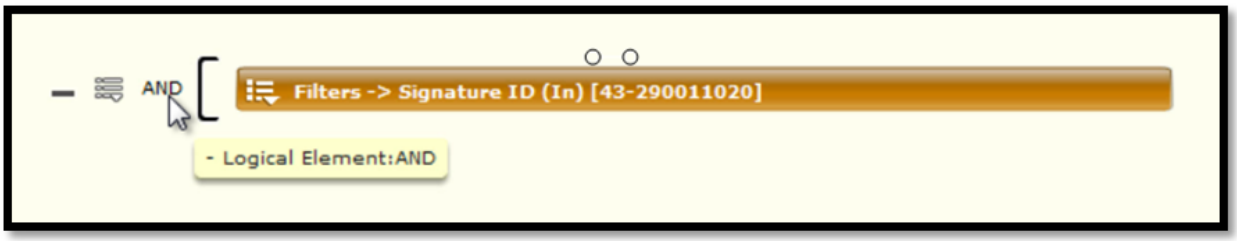
14) Click OK.

15) Click OK one more time. We can see that our filter is added. It will trigger the alarm when the signature ID of an event matches the one we just copied, which is when the Windows security event log is cleared.

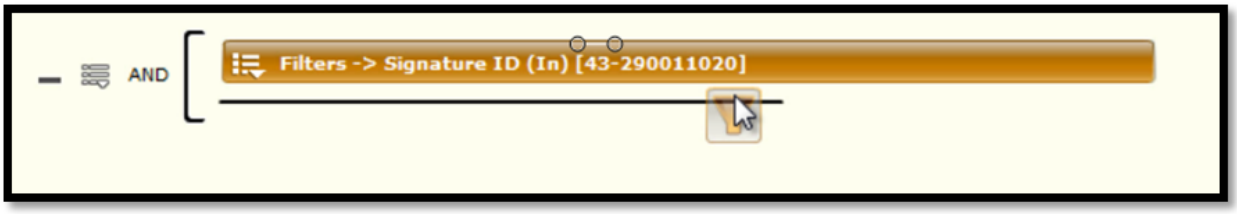


16) But now, let's say we only want to be alerted if this happens on our mission critical servers. So, let's drag and drop the AND logical operator.



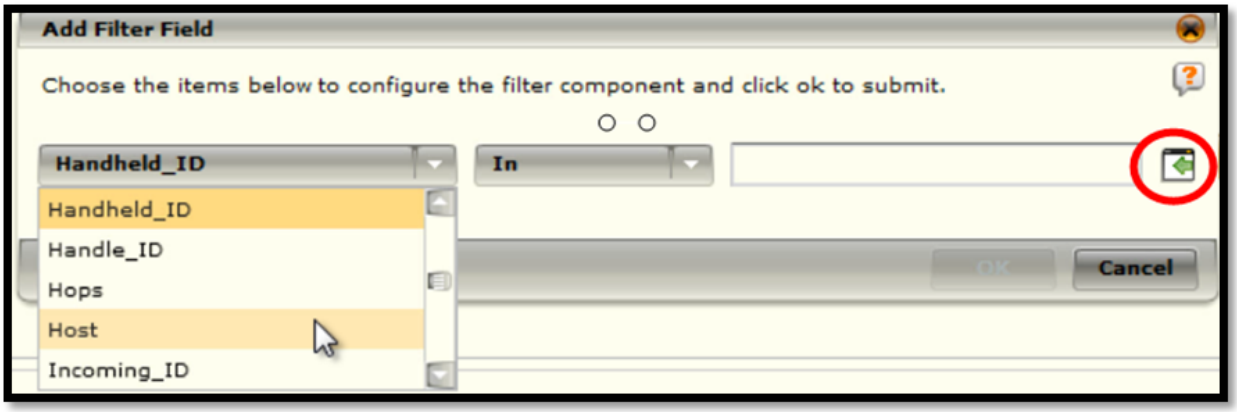


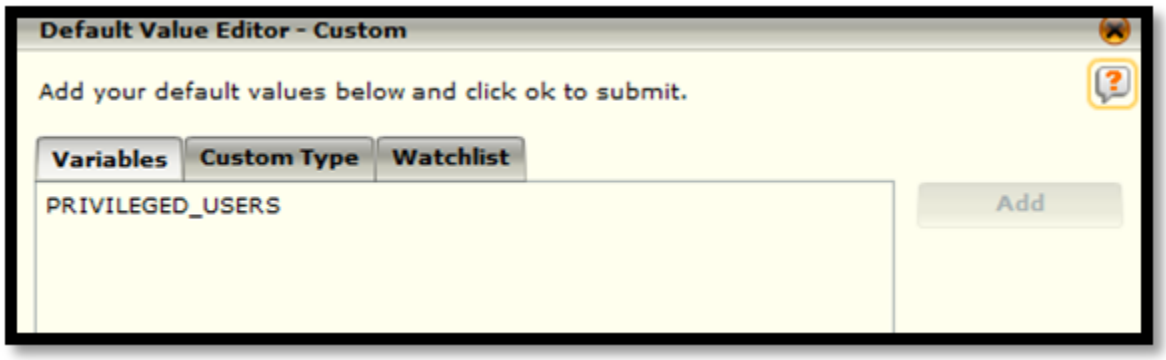
17) To filter on the server name, we need to drag and drop another filter. Let's do that.



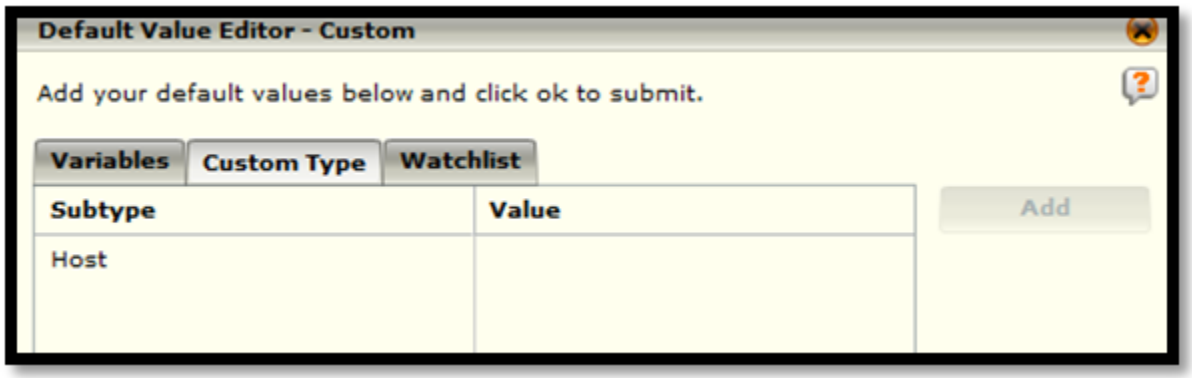
18) A new Add Filter Window opens.

19) This time, we are going to select Host. Click on the little green arrow on the right to define the host value to match.

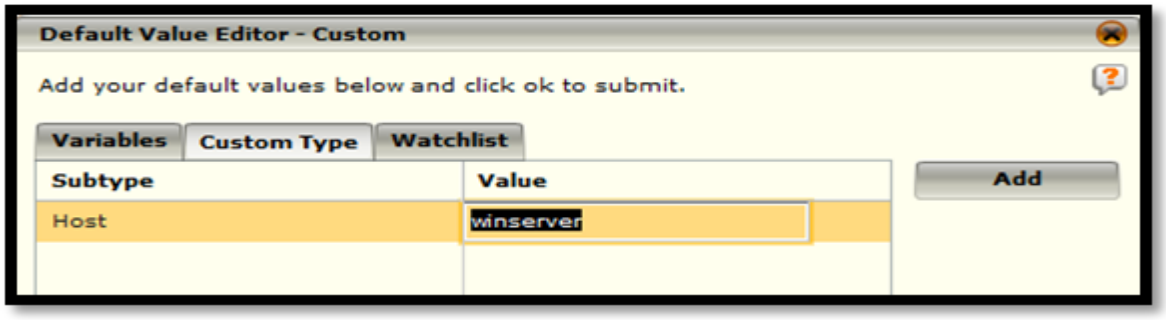




20) In this case, we know that Host is a custom type, so we'll click on the custom type tab.



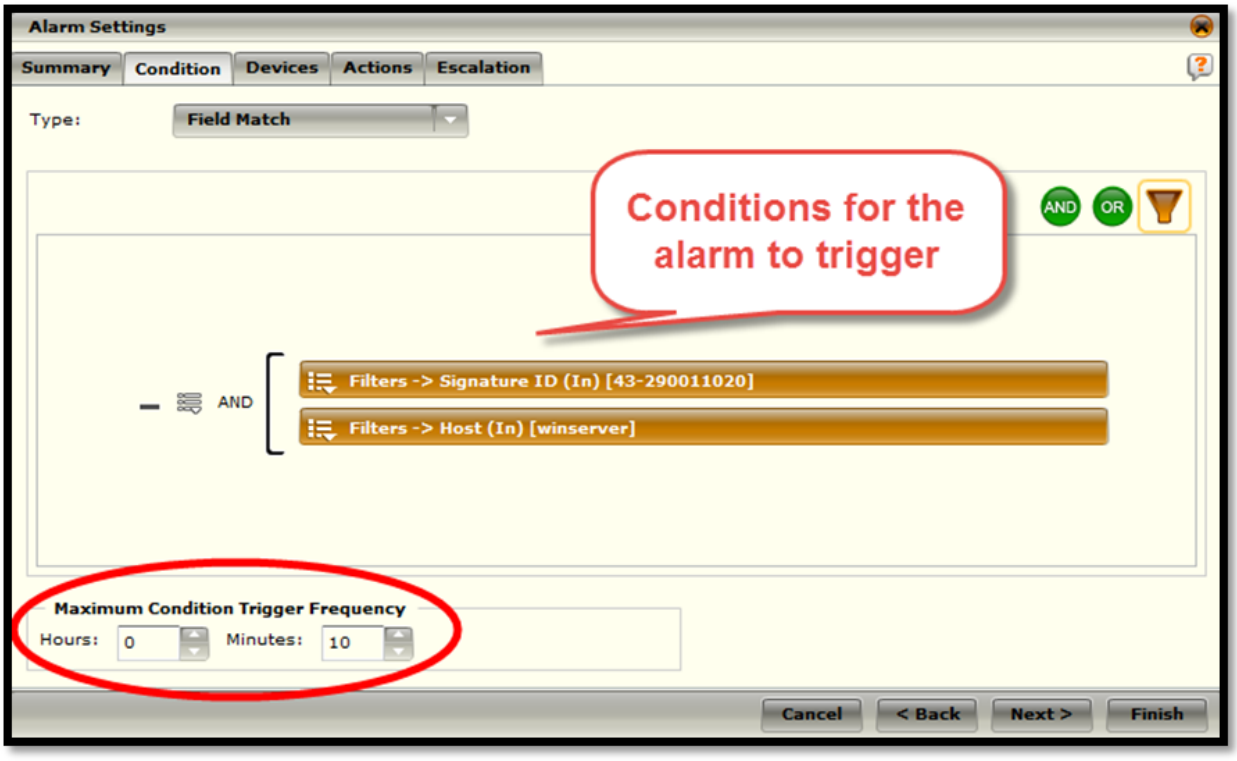
21) Click in the value column next to Host, and enter the name of your server. In our case, our server name is "Winserver," so, that's what we will enter here.



22) Click Add and click OK. Click OK again.

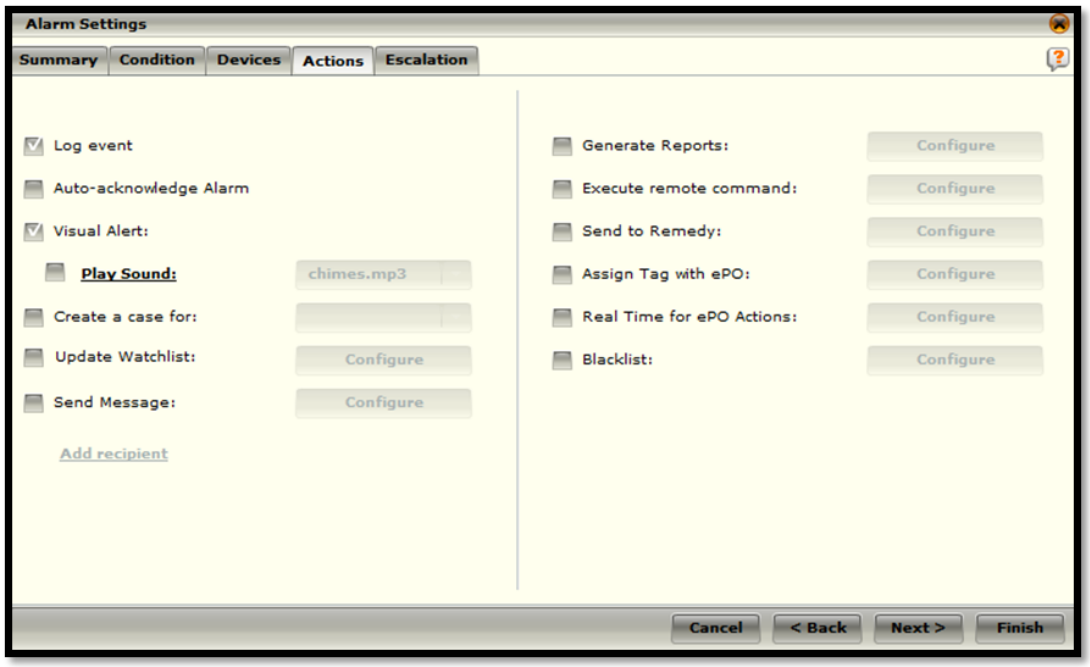
Our two conditions have been added. The event's signature ID will have to match a window log cleared event and the host will have to be name "Winserver."

In the Maximum Condition Trigger Frequency field, you can select the amount of time to allow between each condition to prevent a flood of notifications. Each trigger will contain the first event that matches the trigger condition within the trigger frequency period. If you set it to zero, all matching events will generate an alarm.

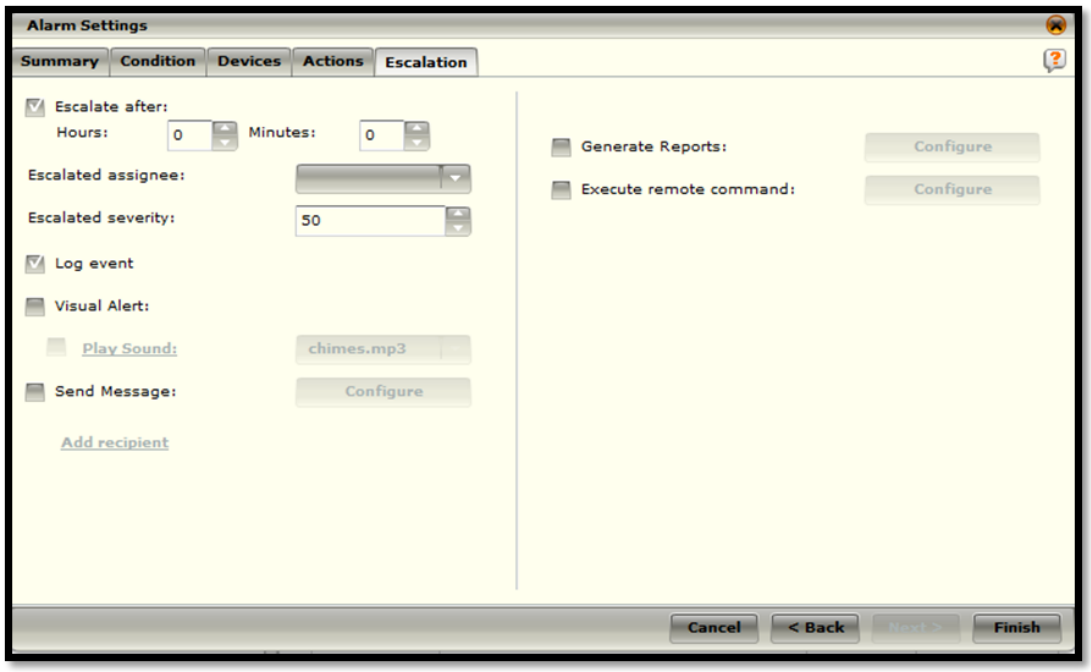


23) Click Next. We are going to check the alarm for our Receiver. That means the alarm will be enabled only for events coming through this receiver. You can check the other devices of your choice if you want to enable this alarm on them too. This also means that the alarm will trigger as soon our receiver sees it, without even being sent to the ESM.

24) Click Next. Now we are going to select what happens when the alarm triggers. We are going to choose to log the event and have a visual display on our console.

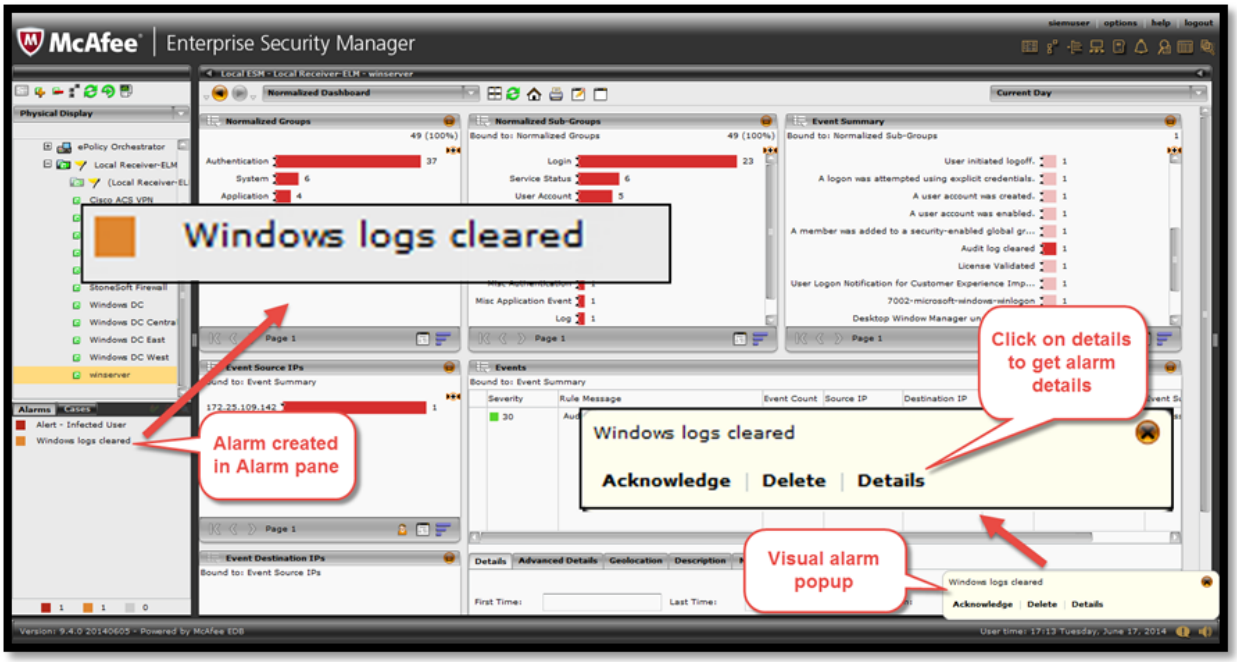


25) Click next. Here we can setup an escalation process. We are going to keep the defaults.



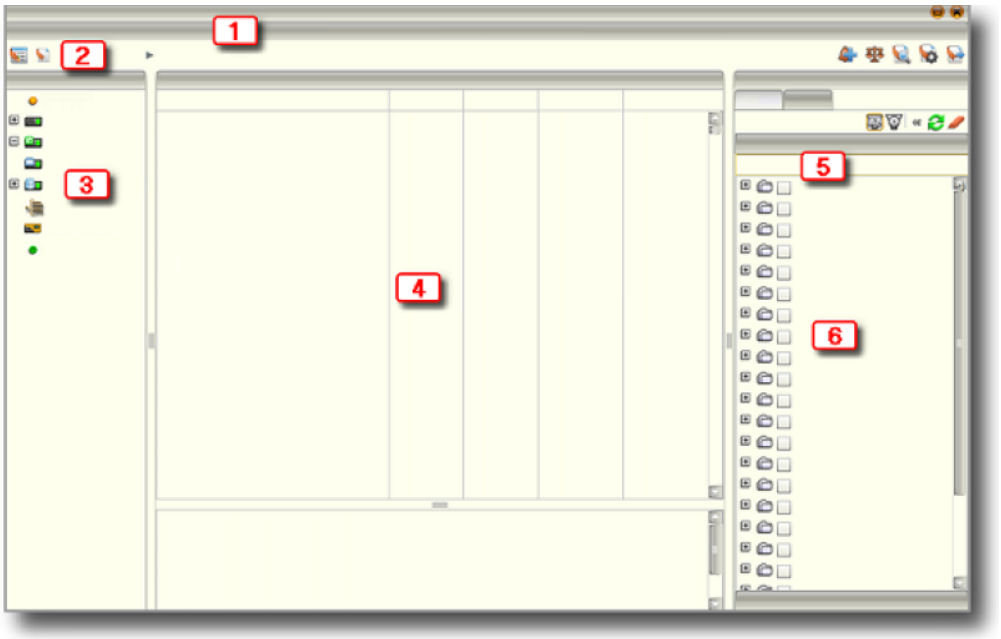
Triggered Alarms

When an alarm is triggered, you will get a pop-up on the ESM console (as long as the visual alert option is checked in step 24 above) and it will be show in the alarm pane in the lower left corner of the screen.



Policy Editor

The Policy Editor window is shown below with the layout. Policy editor is where rules can be viewed, added, deleted, turned on/off, or the severity level adjusted.



1	Menu bar	4	Rule display
2	Bread crumb navigation pane	5	Tag search field
3	Rule types pane	6	Filters/Tagging pane

Cases

The ESM case manager allows you to assign and track work items and support tickets associated with events.

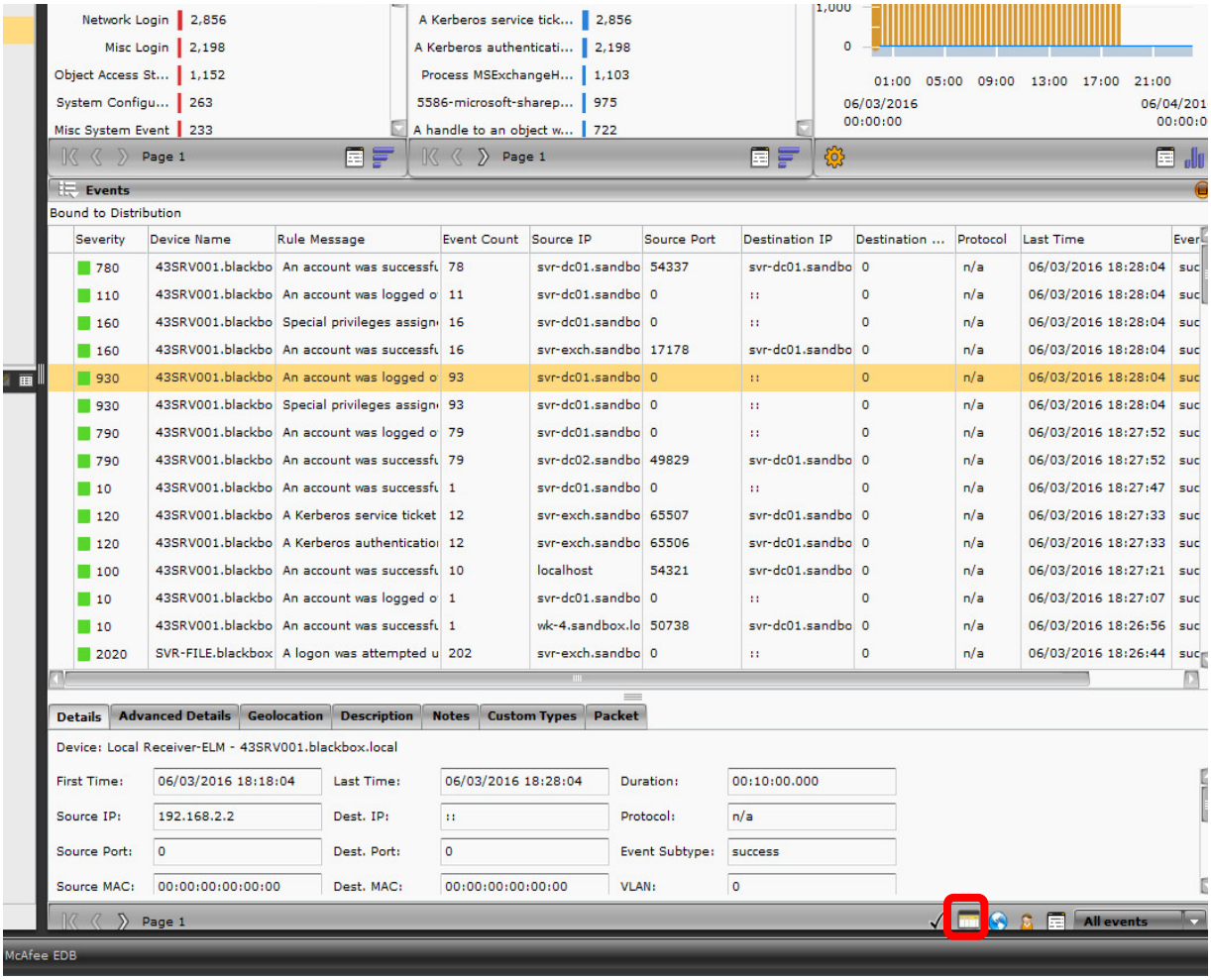
There are five ways to add a case:

- On the Case Management view
- On the Cases pane, without linking to an event
- On the Event Analysis view, linking it to an event
- When you set up an alarm

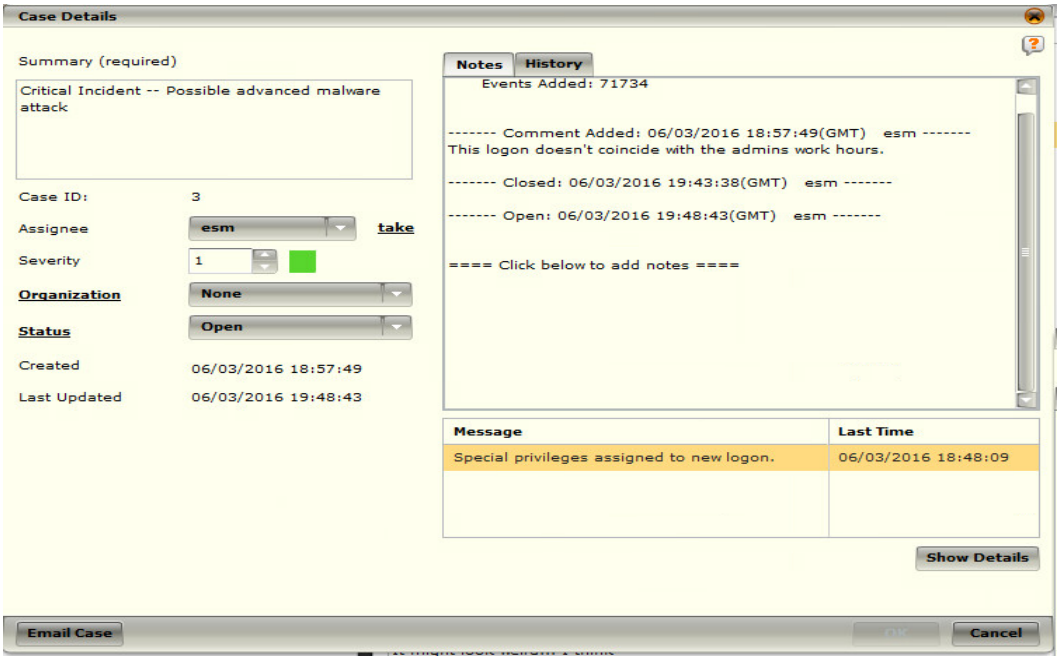
We will only discuss the first two methods.

Create new Cases

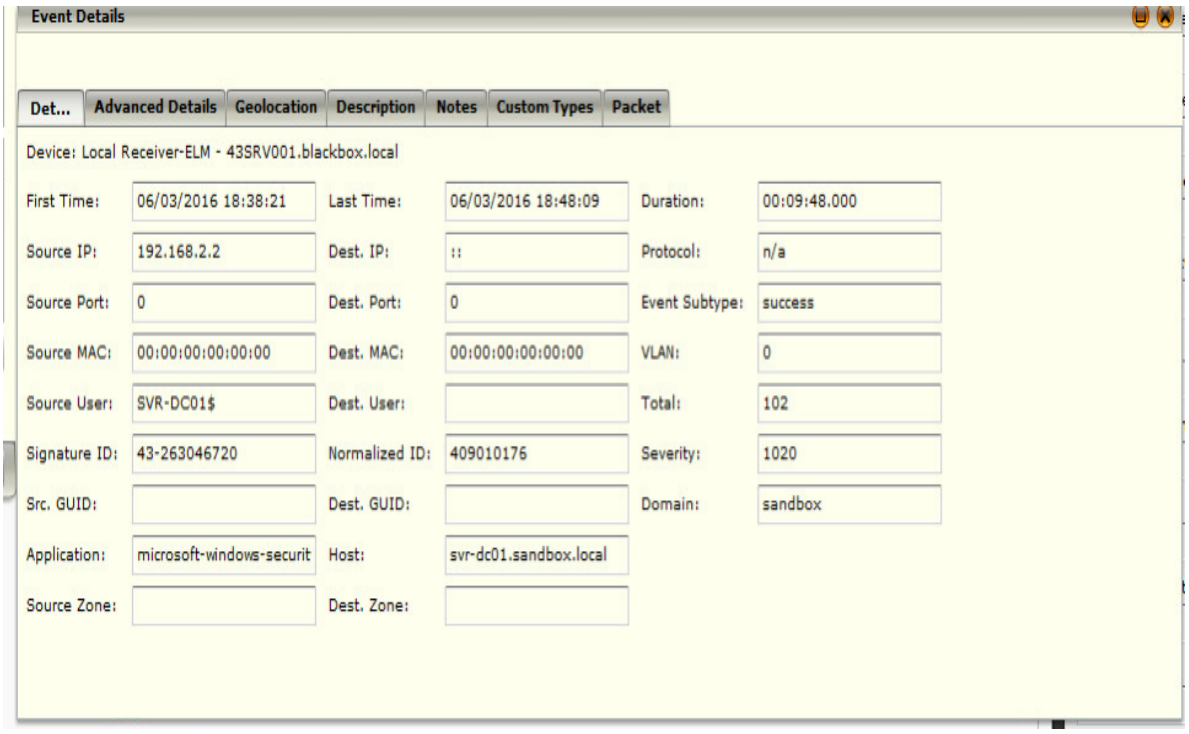
1) In the Events pane (shown below), highlight an entry of interest and click on Cases icon.



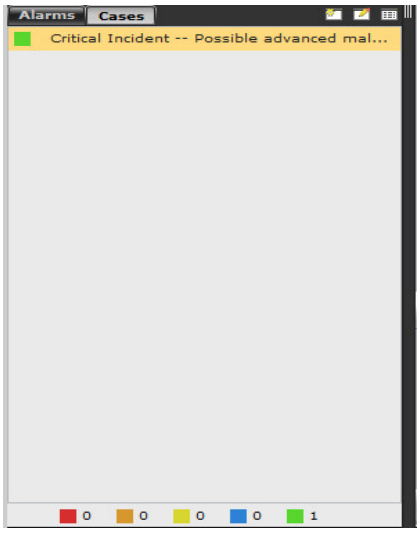
2) Click Create a New Case.
3) Enter a summary, assignee, severity, status, and notes as shown below.



Note: By clicking the Show Details bottom in the above image, you will be able to see the detail events leading to the generation of the Case.



4) Click OK.
5) The Case will now show up in the Cases Pane in the bottom left corner of the screen, as shown below.



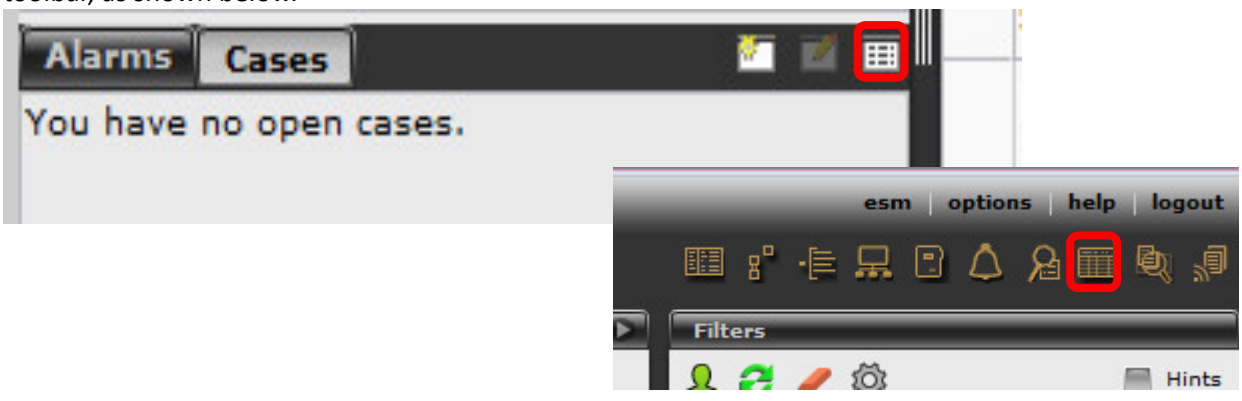
6) Double-click the event to open it. Once open, adjustments can be made to the case including additional notes, changing the assigned person, severity level, and status.

Note: You can also create a Case first and then go back and link events to it which is not the recommended way but it is possible.

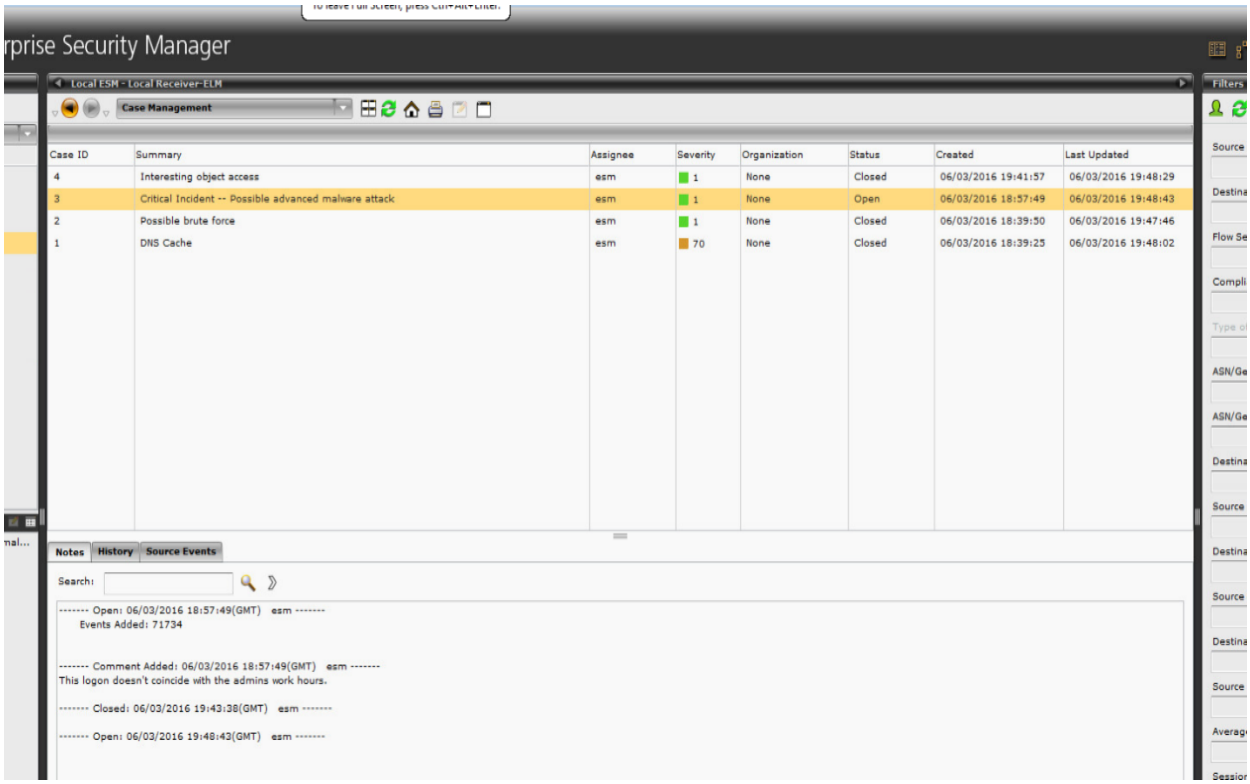
Case Management

Case Management will allow you to view all Cases in a holistic view. You can also reopen a Case and alter any details pertaining to it.

1) Open to Cases Management window by way of the Cases pane in the lower left corner or via the toolbar, as shown below.



3) You will be presented with a list of all Cases. From here you can see the notes, history, and source events for each Case. You can also open any closed Cases.

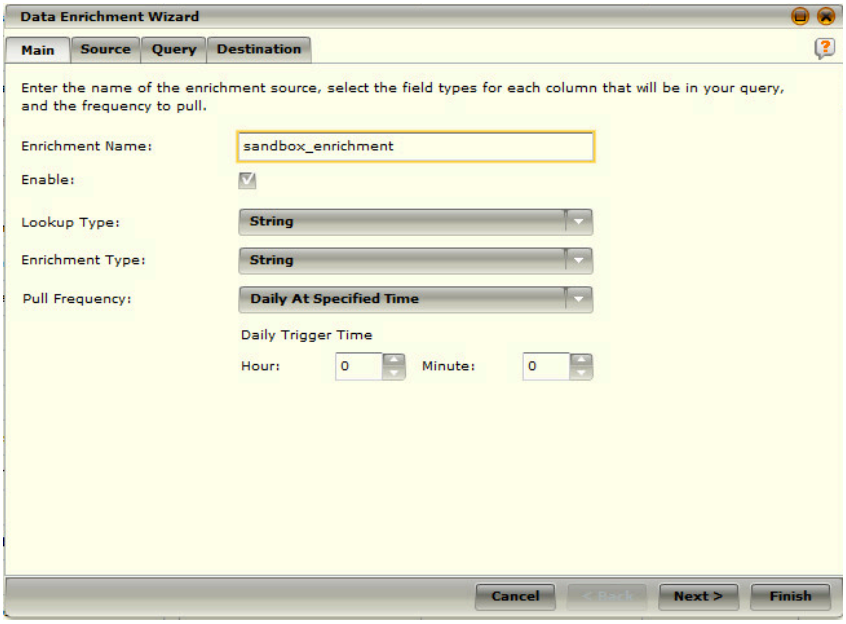


Data Enrichment

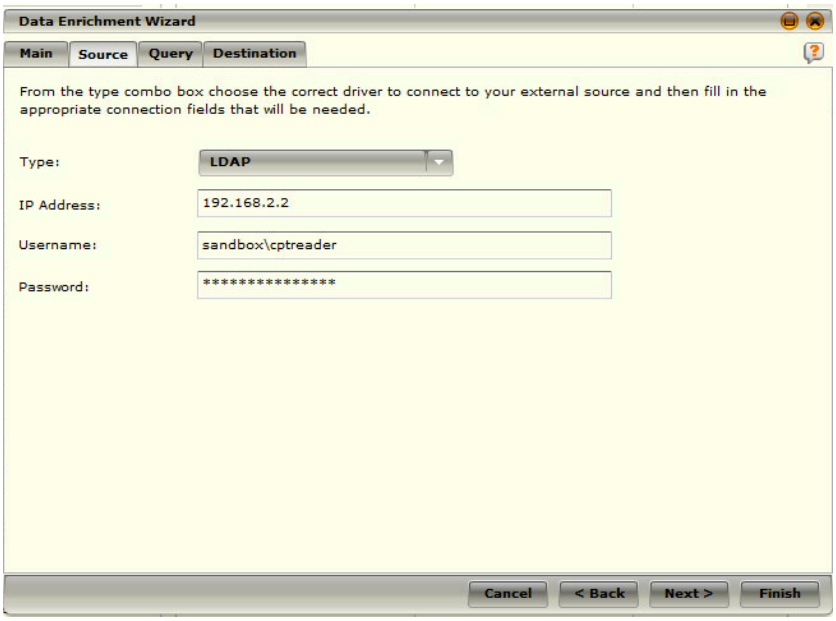
The Data Enrichment feature of the ESM allows you to enrich events with context that is not in the original event sent by the upstream data source, such as an email address, phone number, or host location information. This data becomes part of the parsed event, and is stored with the event just like the original fields. There is a wide range of uses for Data Enrichment but we will only highlight one, which is of great use for defenders. In example below, we will use it to populate full user display names in Windows events.

Pulling from Active Directory

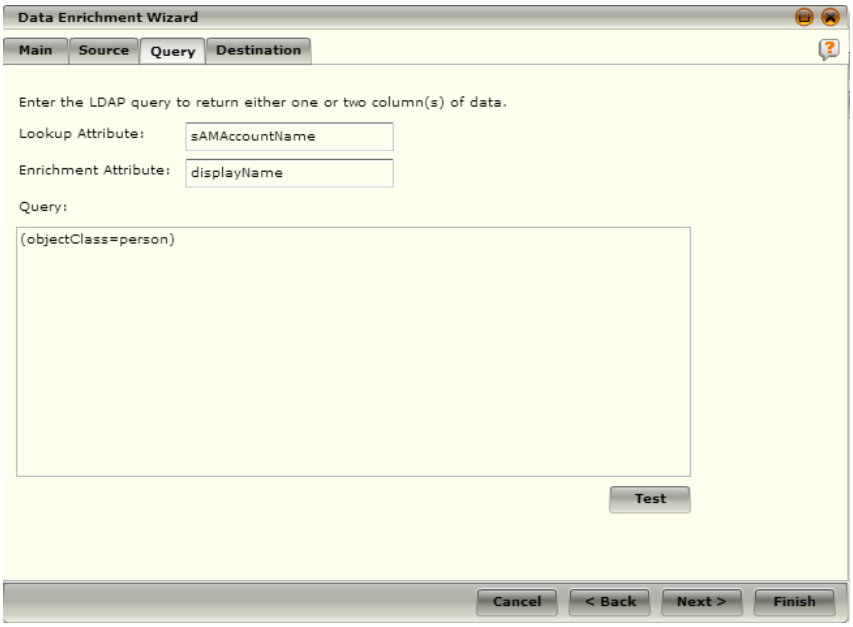
1) Select System Properties > Data Enrichment.
2) Click Add to create a new Data Enrichment.
3) Input a name; change the Lookup and Enrichment Type to String. Adjust the Pull Frequency as needed but daily should suffice.

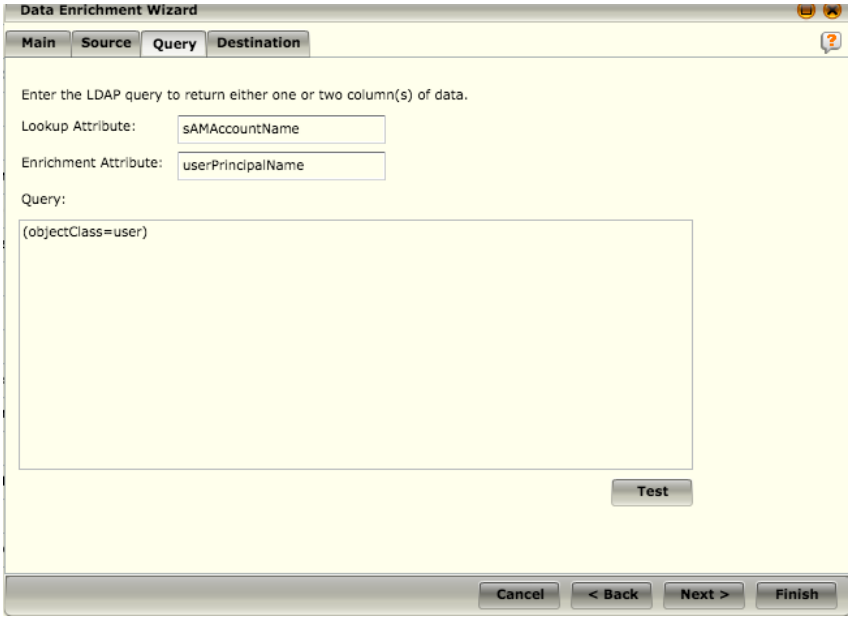


4) Define the Active Directory (or LDAP) Source. The username and password supplied must have read access to user objects in Active Directory.

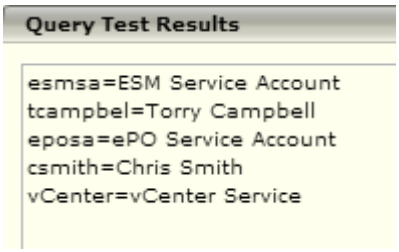


5) Create a query. The first image an example of how to pull the Display Name and the second image depicts pulling the username. For this example, we will be using the Display Name. Once complete, click the Test button.

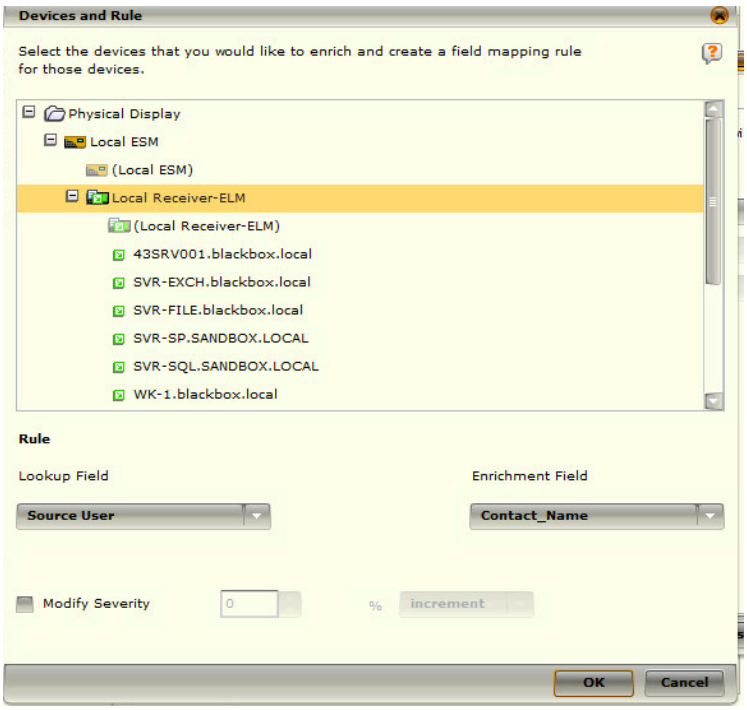




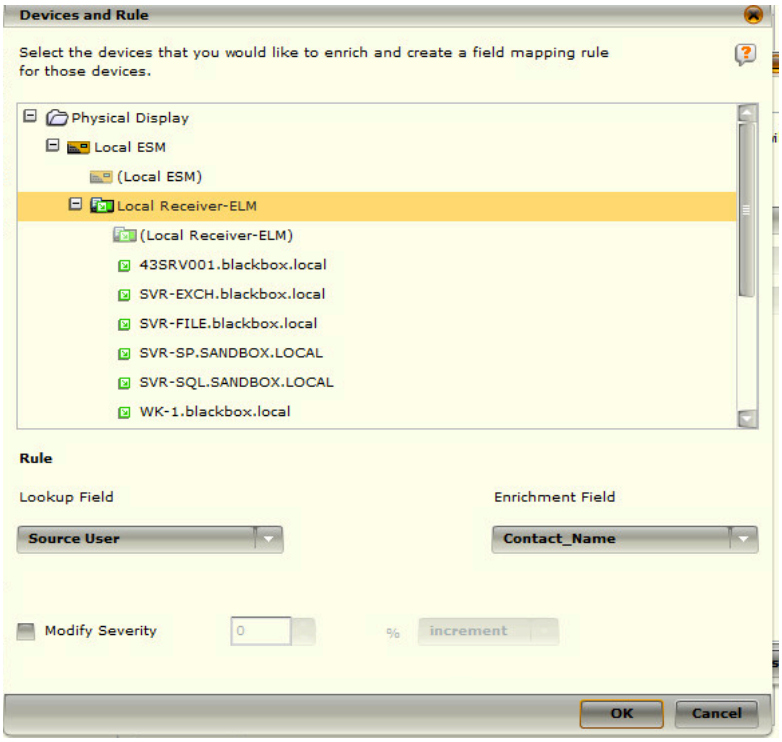
If the test is successful, it will return something similar to the below image. The test function only returns a maximum of 5 values, regardless of the number of actual entries.



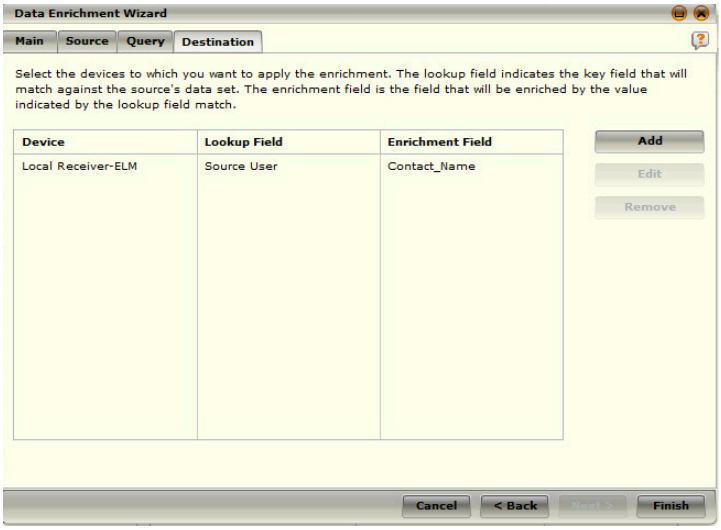
6) Click Next.
7) Click Add to add a Destination.
8) Select the Receiver as shown below.



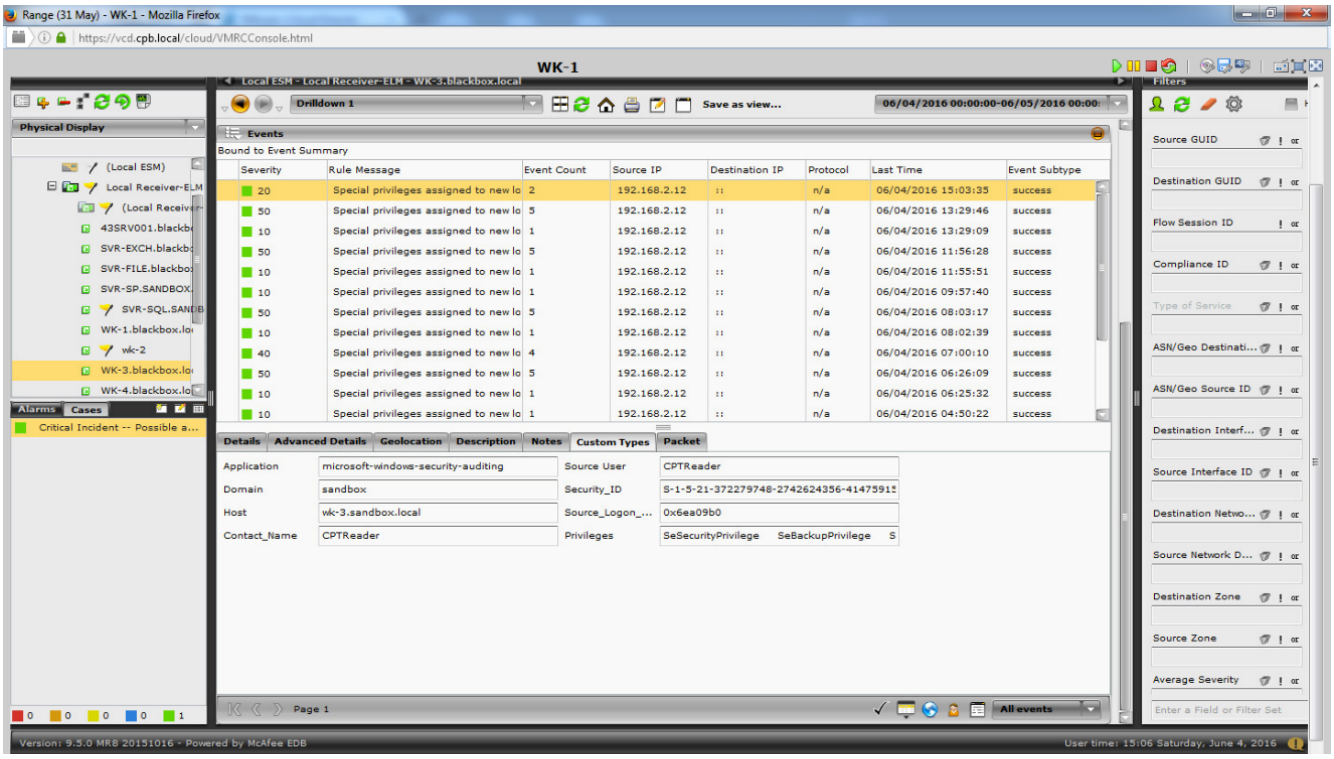
9) Select the Lookup Field. In this case it will be the Source User field. The lookup field is the value that exists in the event, which we will use as the index for our lookup. Select the Contact_Name for the Enrichment Field.



10) Click OK and you will see the below image.



11) Click Finish to save.
12) Click the Write button in the bottom left corner.
13) After complete, click Run Now or the enrichment values will not be retrieved from the data source until the 'Daily Trigger Time' value set in earlier is reached.
14) An event enriched as above will have the Full Name written into the Contact_Name Field. Notice below that the information is populated for user CPTReader.



Cyber Threat Manager

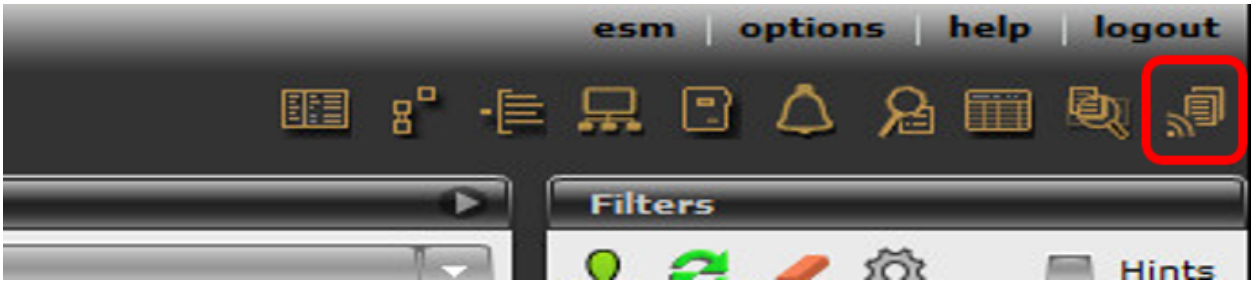
The Cyber Threat Manager allows the McAfee ESM to receive and parse Indicators of Compromise, or IOCs, and display them in the dashboards. There are various ways to pass the McAfee ESM IOCs but we will only address STIX files. You can accomplish importing STIX files manually or through a feed.

Note: To convert an .ioc to .xml, check out openioc-tostix on github located at https://github.com/STIXProject/openioc-to-stix.

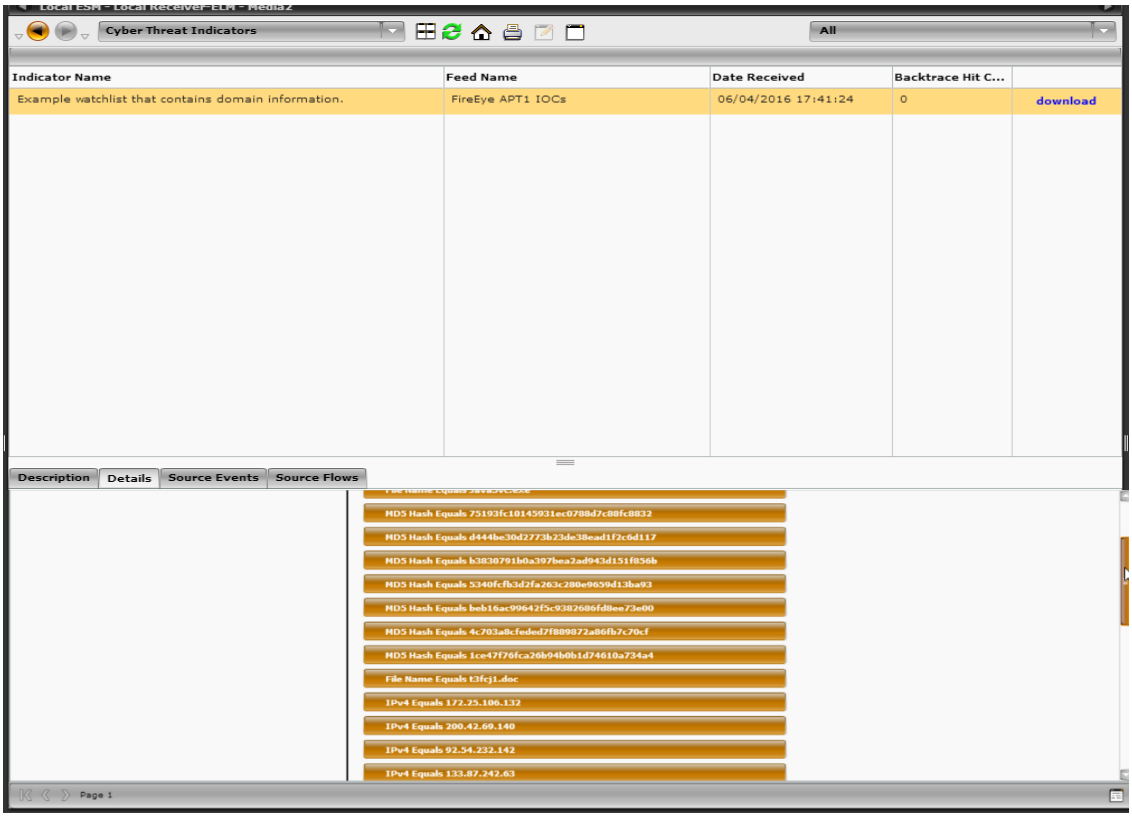
Setup the Cyber Threat Manager

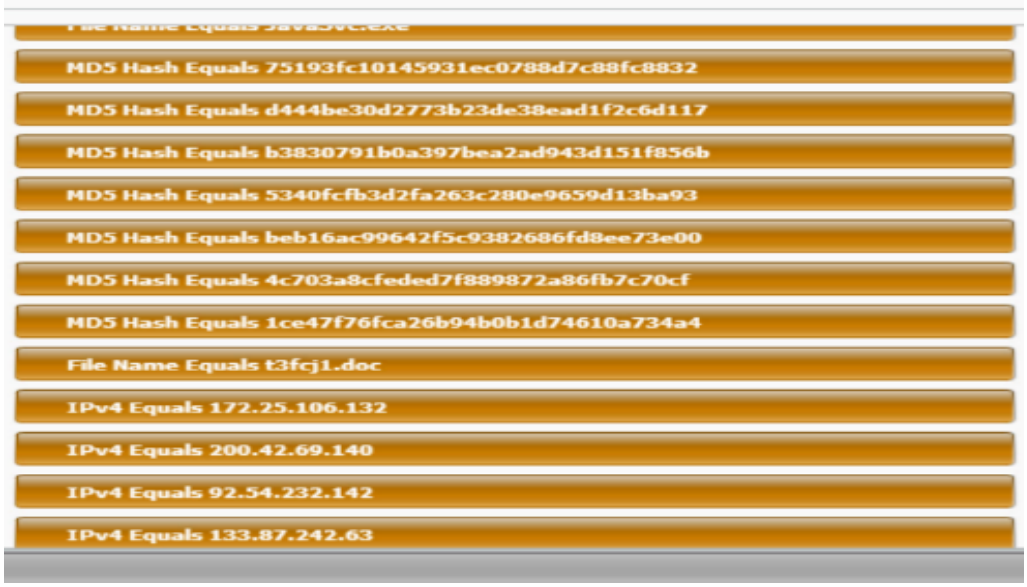
1) Click on the System Properties and then select the Cyber Threat Feeds section.
2) Click Add.
3) Give the entry a name.
4) Click Next.
5) For Source tab, select “Manual” for the Type.
6) Click Next.
7) It is recommended that you link these IOCs to a watchlist by selecting an Indicator Type and specifying a watchlist. You can skip this step if need be and revisit it at another time. Without a watchlist that the IOCs can populate, having IOCs do nothing.
8) Click Next.
9) On the Backtrace tab, this is where you can input how far back to search your data for the IOCs you are uploading. You can also setup what actions to take upon firing.
10) Click Finish.

11) Click Upload.
12) Browse to the location of your STIX formatted .xml file and select it.
13) Click Upload to actually upload it to the system.
14) Once you are presented with a successful upload message, click Close.
15) Click OK to close out the Cyber Threat Manager window.
16) Click on Cyber Threat Indicators button on the toolbar as shown below.



17) Your newly uploaded indicators will be present as shown below. From here, you can see how many backtrace hits there were, the feed name, date received, and have the ability to download it. You can see the IOC in a more human-readable format. An image depicting all of these items is shown below.





External SIEM Communications

Receiving Data from another SIEM

Often times defenders will find that a supported organization may have a SIEM or log aggregation system in place. If that is the case, we can either leverage their system use it for the mission or become a downstream SIEM and receive data from them. To do so, a data source will be needed for syslog.

Setting data source is addressed in the Adding Linux or Other SIEM Data Sources section of this document.

Sending ESM Data to another SIEM

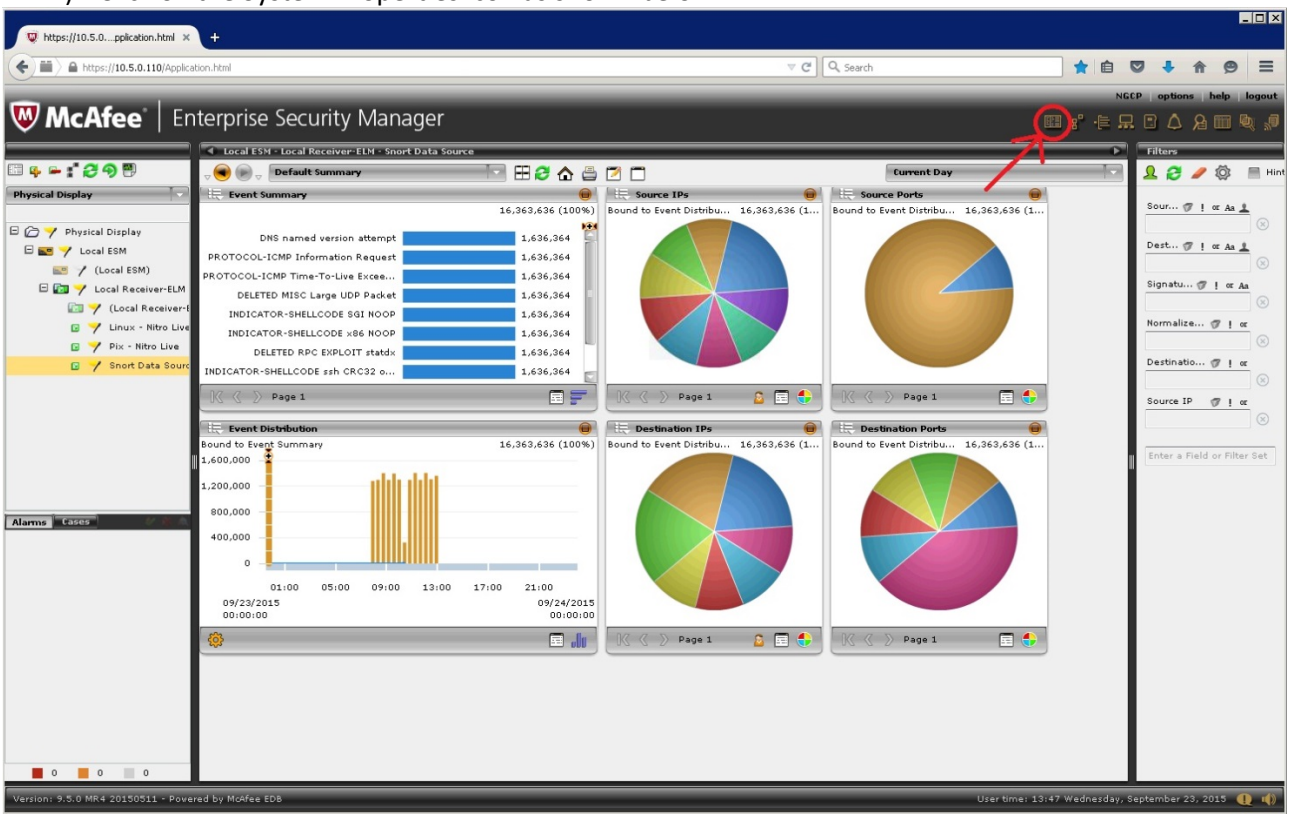
There may be times where the data we receive will be requested by other entities. Whenever that may be, ESM has the built-in capability to send data to other systems via syslog. Some of the common systems are Splunk, ArcSight, Graylog, and ELK.

Forward Parsed Data

Using this method sends data directly from the ESM. This applies to parsed and aggregated events. The benefits are that you can select what data is sent to another SIEM of syslog server. The disadvantage is that the format will be different from the original event and may require additional parsing on your other SIEM.

To forward data to another system, do the following:

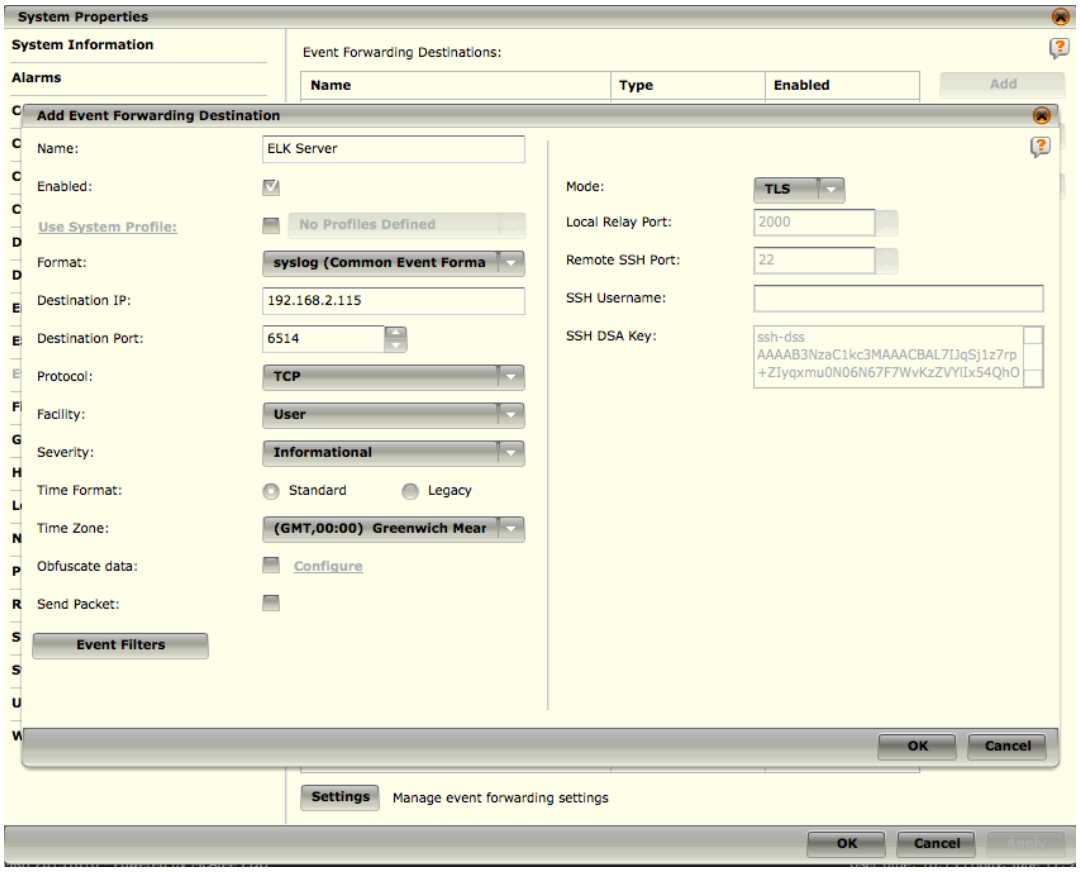
1) Log onto the McAfee ESM.
2) Click on the System Properties icon as shown below.



3) Select the Event Forwarding option.
4) Click Add to create a new Event Forwarding Destination.
5) Input data for the fields below:

- Name - Event Forwarding Destination.
- Ensure that it is enabled.

- Select syslog (Common Event Format) from the Format drop down menu.
  Note: Depending on the distant system, you may have to select a different format.
- Enter the destination IP.
- Enter a destination port (514 or 6514 are suitable ports).
- Select TCP from the Protocol drop down menu.
- Select User from the Facility drop down menu.
- Select Informational from the Severity drop down menu.
- Select Standard as the Time Format.
- Select GMT as the Time Zone.
- Ensure that the Send Packet option is checked. Select TLS from the Mode drop down menu.



6) Click OK.
7) Click the Settings button at the bottom of the System Properties screen.
8) Ensure that the “Event Forwarding Enabled:” option is checked, and then click OK.
9) Click OK to complete the configuration.

Forward Original Syslog Data

Using this option will send the raw unparsed packets that the receiver receives to another server and is more of a pass-through. It will also parse the events locally on the ESM.

1) Go to Receiver properties.

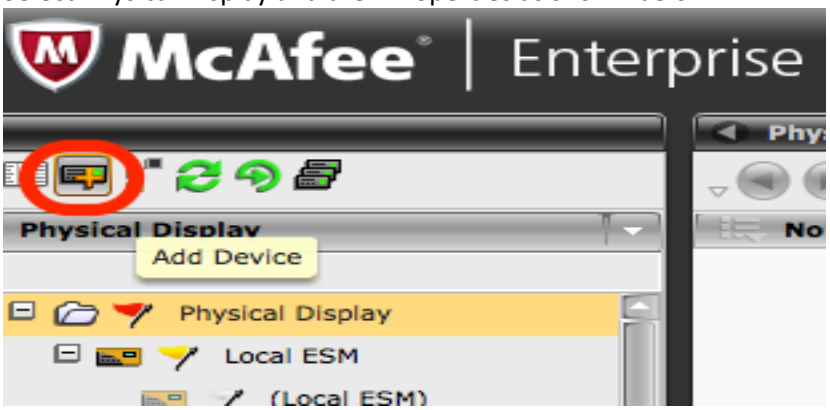
2) Click on Receiver/ELM Configuration > Data Archival.
3) At the bottom of the window, enable Syslog Forwarding and fill in the necessary information.

Sending Data to another ESM

Distributed Enterprise Security Manager (ESM) Event Forwarding

Distributed ESM is used to receive or send events from or to other ESMs.

1) Select Physical Display and then Properties as shown below.



2) Select Distributed ESM.
3) Click Next.
4) Click Yes to the warning.
5) Enter a name for the data source you will be communicating with.
6) Click Next.
7) Input the IP, username, and password of the data source you will be communicating with. Don't change the port!
8) Click Next.
9) Click OK when the prompt appears saying the device was successfully added.
10) Click Finish.
11) Select the ESM you just added and click properties.
12) Click Filters.
13) Click the icon on the Device ID line.
14) Select the feeds you want to be seen by the other ESM.
    Note: You must select a filter to send!
15) Click OK.

Advanced Syslog Parser (ASP)

Compared to other SIEMs, the advanced parser on ESM is pretty straightforward and user friendly. The best guide available to make a custom parser can be found at the below link. The biggest thing needed is a sample of the logs you wish to build the parser for. This is because as you are building the regex parser, ESM will assist you by highlighting the applicable field.

https://kc.mcafee.com/corporate/index?page=content&id=PD24926&actp=RSS

Bro IDS Log Parser

Utilizing the above directions and looking at the existing Bro DNS Log parser, the only thing needed is the regex used to parse the data from the log, which can be found below. As I make more parsers for the other logs, this document will be updated.

The below will grab the time, uid, src_ip, src_port, dst_ip, dst_port, protocol, services, duration, conn_state, and history from the conn log.

Conn log:

(?P<time>\d+\x2e\d+)*\x09(?P<uid>[0-9a-zA-Z]+)\x09(?P<src_ip>[^\x09]+)\x09(?P<sr
c_port>\d{1,5})\x09(?P<dst_ip>[^\x09]+)\x09(?P<dst_port>\d{1,5})\x09(?P<protocol
>[^\x09]+)\x09(?P<service>[^\x09]+)\x09(?P<duration>\d+\x2e\d+)\x09(\d+)\x09(\d+
)\x09(?P<conn_state>[0-9a-zA-Z]+)\x09(\w+)\x09(\w+)\x09(\w+)\x09(?P<history>[0-9 a-zA-
Z]+)\x09(\d+)\x09

The below will grab the time, uid, src_ip, src_port, dst_ip, dst_port, src_mac, and assigned_ip from the DHCP log.

DHCP log:

(?P<time>\d+\x2e\d+)*\x09(?P<uid>[0-9a-zA-
Z]+)\x09(?P<src_ip>[^\x09]+)\x09(?P<src_port>\d{1,5})\x09(?P<dst_ip>[^\x09]+)\x09(?P<dst_port>\d{1,
5})\x09(?P<src_mac>[^\x09]+)\x09(?P<assigned_ip>[^\x09]+)

Annex A: PowerShell ESM Import Script

On my github (www.github.com/wiredpulse), I have a PowerShell script that I wrote that saves a list of all computers in the domain and inputs them into a CSV. After the script is ran, open the file with Notepad or Notepad++ and save the document with UTF8 encoding.

Annex B: Enabling Windows Auditing

It goes without saying that if auditing isn't enabled, it leaves the organization blind to past and current events. Below we quickly depict where to enable auditing on Microsoft systems, which can be done quickly for a domain using GPO Management. If the system is not part of a domain, the location is still the same but it would need to be done on each system.

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Advanced Audit Policy

Annex C: Troubleshooting

Device Logs

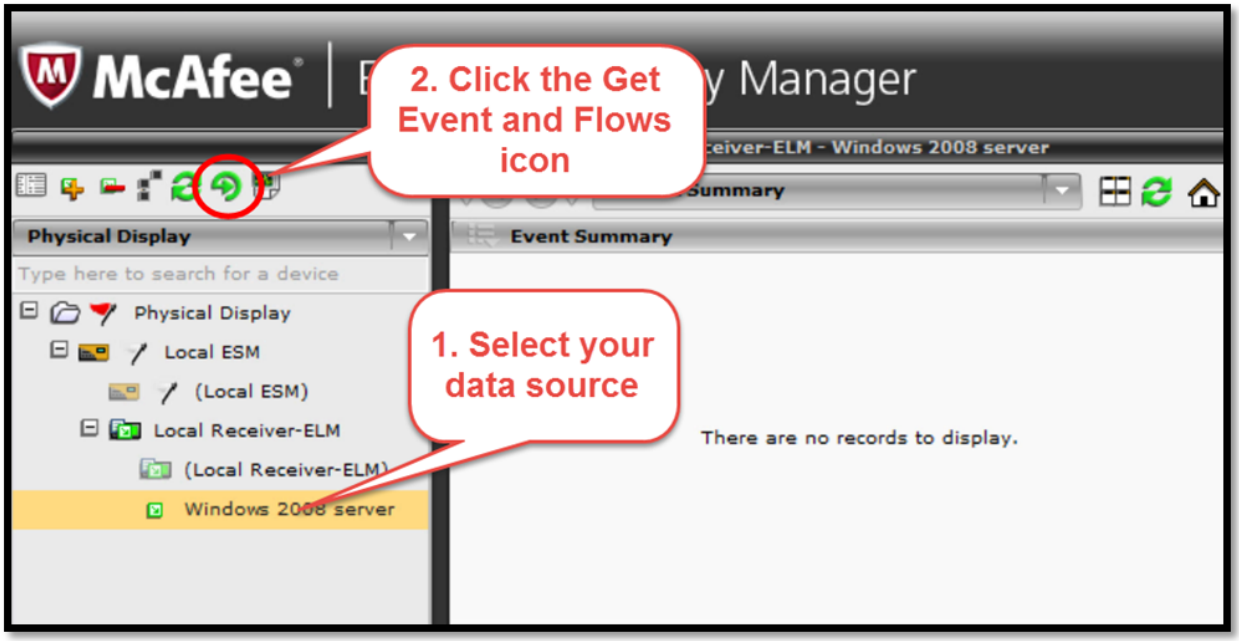
For troubleshooting or just to see what's going within the system, we can view the system logs from the ESM interface. You can also log into the console of the ESM server and look at /etc/messages as well. To look at the logs through the interface, do the following:

1) Open the System properties.
2) Click on System Logs.
3) Provide a timeframe to retrieve.
4) Click View.

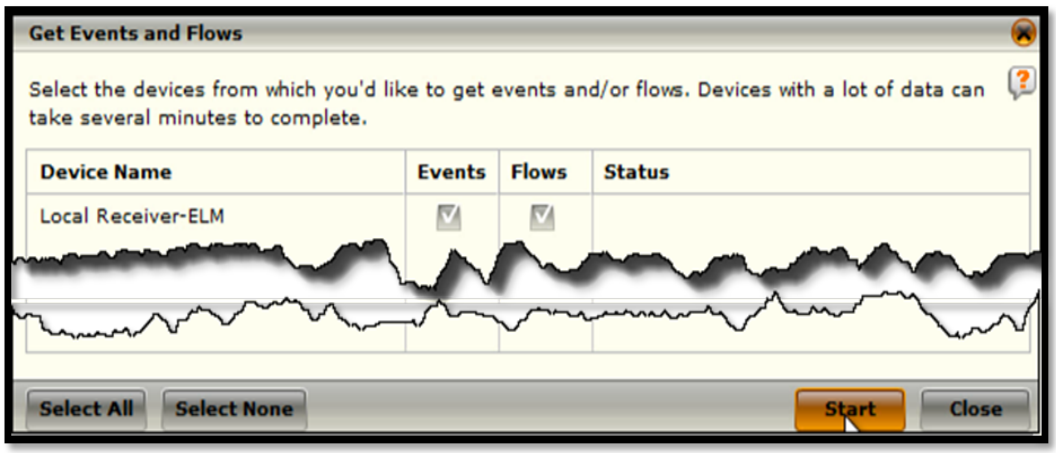
Test if events are being received

After a Data Source has been configured, you can wait the specified interval that you set for ESM to pull logs or we can accelerate the last step by asking ESM to pull those logs right now by doing the following:

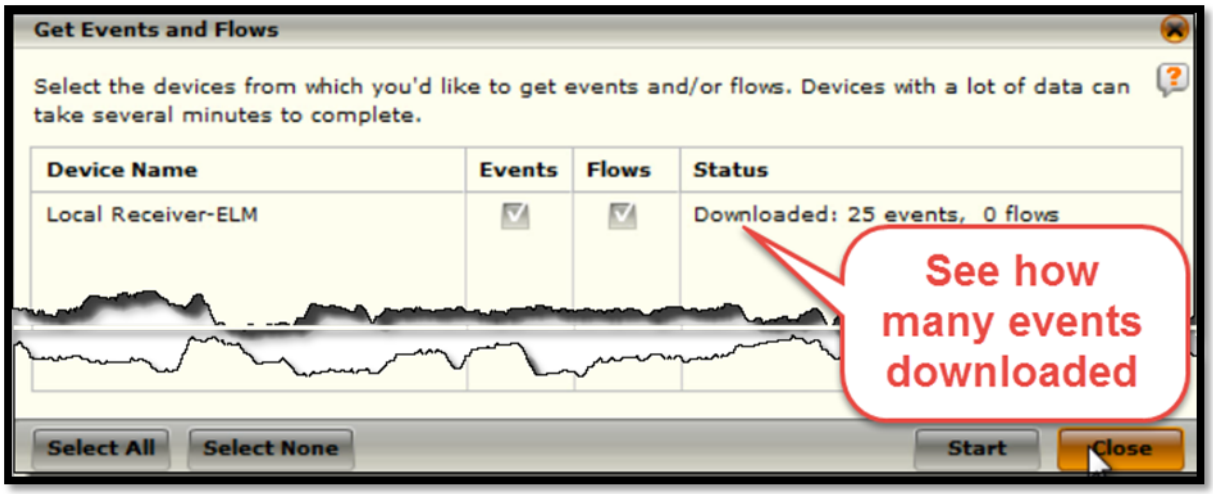
1) Click the "Get Events and Flows" icon in the top left corner of the console.



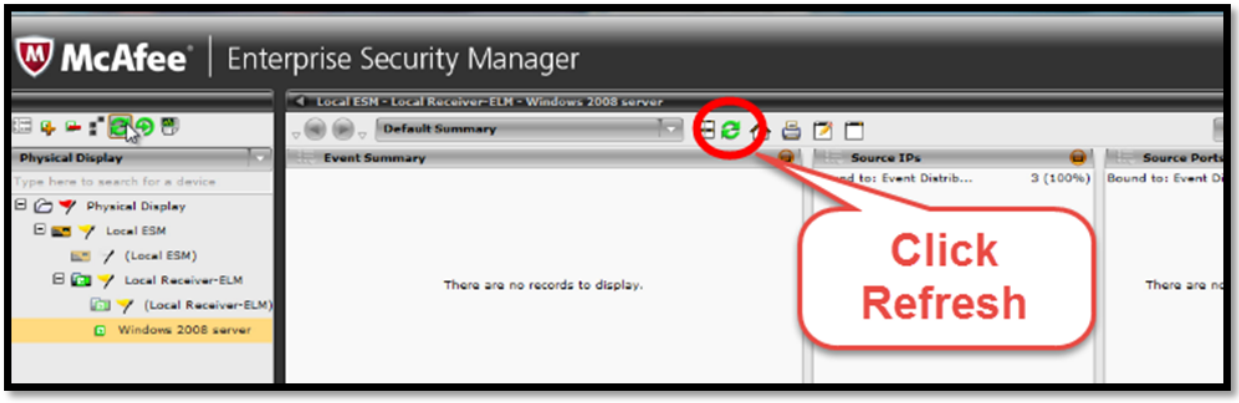
2) The Get Events and Flows window opens. Click Start and the ESM will start downloading events.



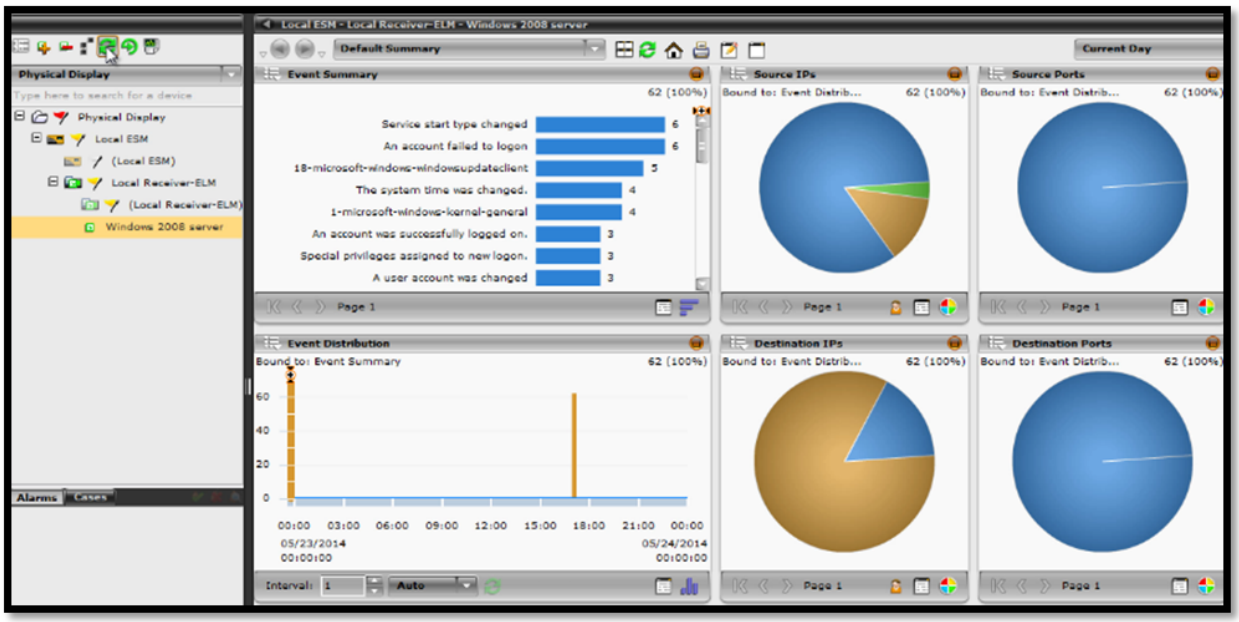
3) When it's done, it will tell you how many events were downloaded. Click Close



4) Click the refresh icon in the top middle of the SIEM console.



5) You should now see windows events in the console.


Local ESM - Local Receiver-ELM - Windows 2008 server
Physical Display
Physical Display
Local ESM
(Local ESM)
Local Receiver-ELM
(Local Receiver-ELM)
Windows 2008 server
Alarms
Cases
Default Summary
Current Day
Event Summary
62 (100%)
Service start type changed 6
An account failed to logon 6
18-microsoft-windows-windowsupdateclient 5
The system time was changed. 4
1-microsoft-windows-kernel-general 4
An account was successfully logged on. 3
Special privileges assigned to new logon. 3
A user account was changed 3
Page 1
Source IPs
Bound to: Event Distrib...
62 (100%)
Source Ports
Event Distribution
Bound to: Event Summary
60
40
20
0
00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00 00:00
05/23/2014 00:00:00
05/24/2014 00:00:00
Interval: 1 Auto
Destination IPs
Destination Ports