

SIEM Collector - PRODUCT GUIDE

Summary

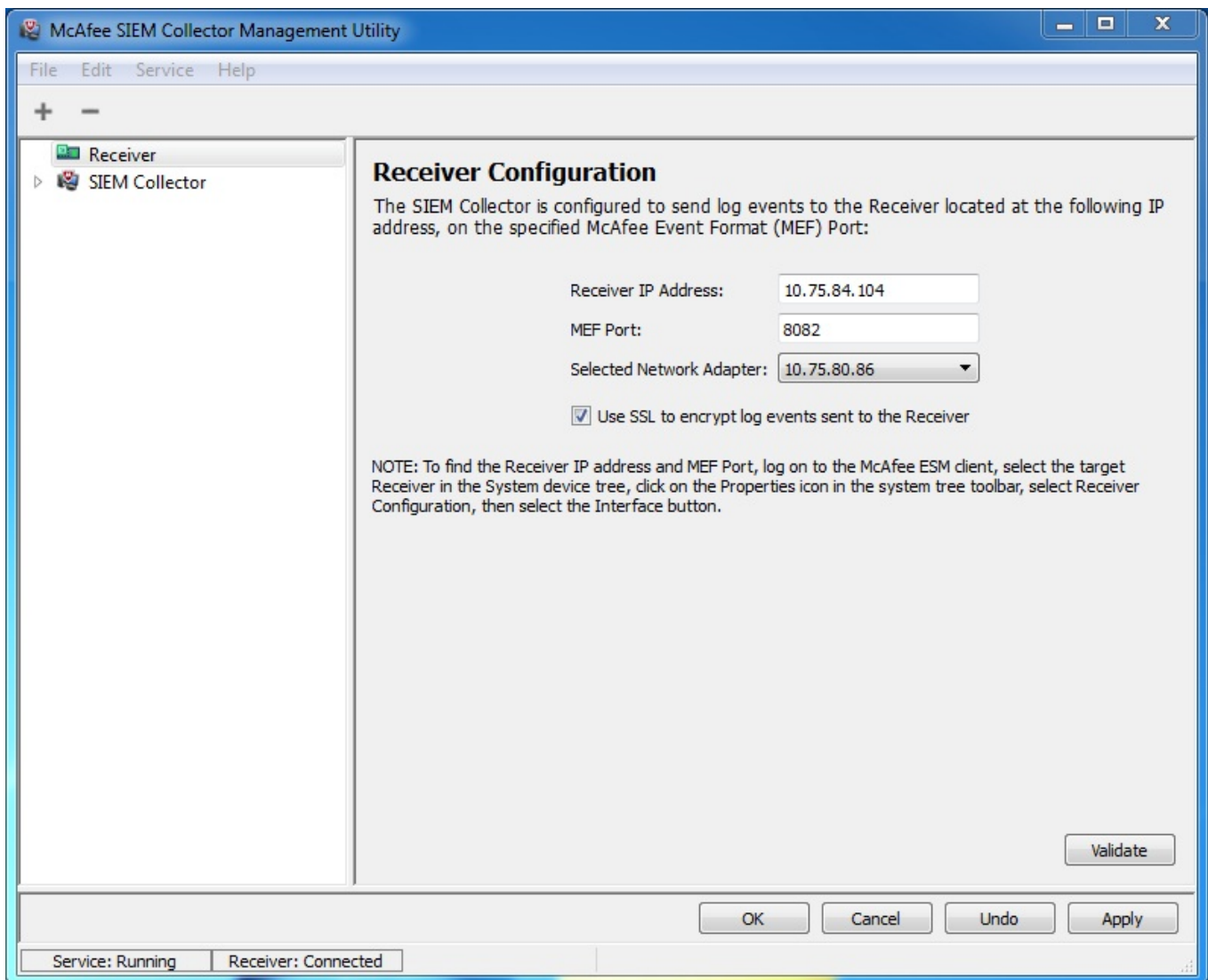
The McAfee SIEM Collector is host-based software that can be configured to send events to a McAfee ESM with a Receiver. The SIEM Collector can be configured to send events from the local Windows machine or from remote Windows machines.

Terms

- MEF - McAfee Event Format: The protocol the SC uses to communicate with a Receiver.
- ESM - Enterprise Security Manager: Interface for the SIEM solution.
- EVT(EVTX) - A file extension for files created by the Windows Event Viewer. .evt is the older format and .evtx the newer.
- SIEM - Security Information Event Management
- DNS - Domain Name Server
- MSSQL - Microsoft SQL Server
- WEF - Windows Event Forwarding.

RECEIVER CONFIGURATION

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.

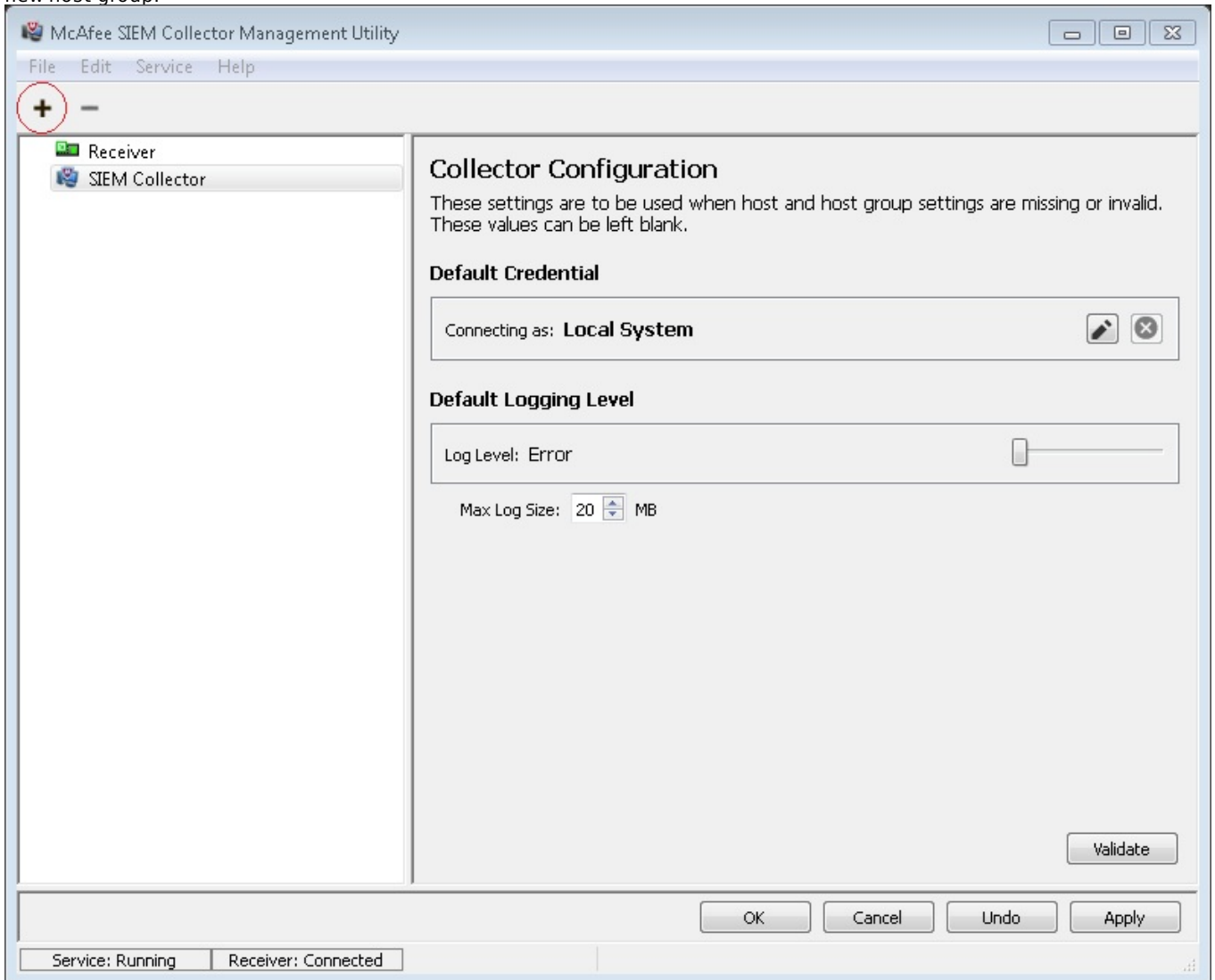
Using SSL to encrypt log events sent to the Receiver:

If you want the event logs to be encrypted using SSL, this box should be checked. If you do check the "encrypted" checkbox, you should also check the "Use encryption" checkbox for each receiver datasource you create. (See Clients section for more help with encryption and encryption with host IDs)

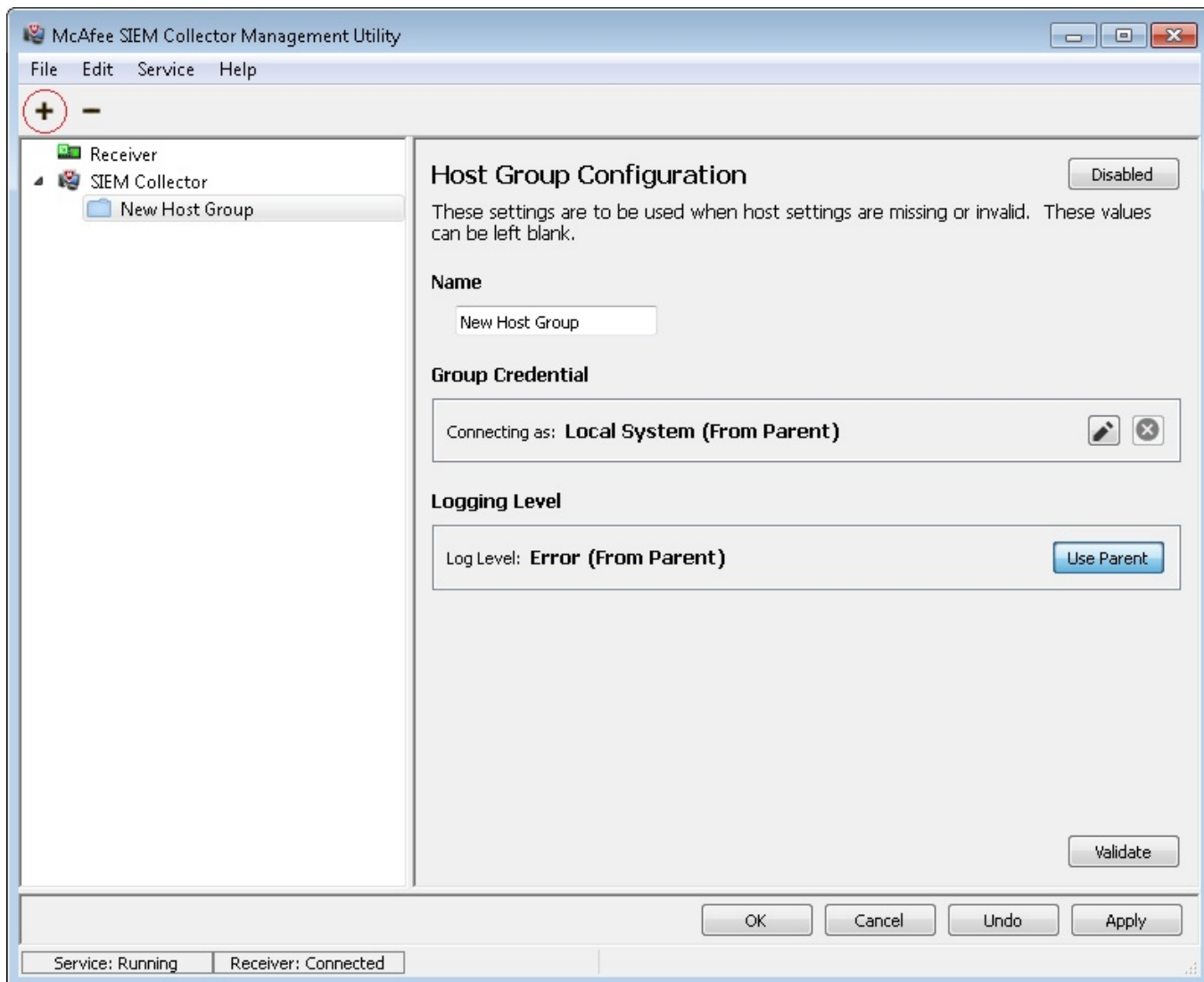
Whenever a change to one of these fields is made, click Apply to save the changes and keep the Utility open or click OK to save the changes and close the Utility. Clicking either of these buttons validates settings and restarts the service if it is running.

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.



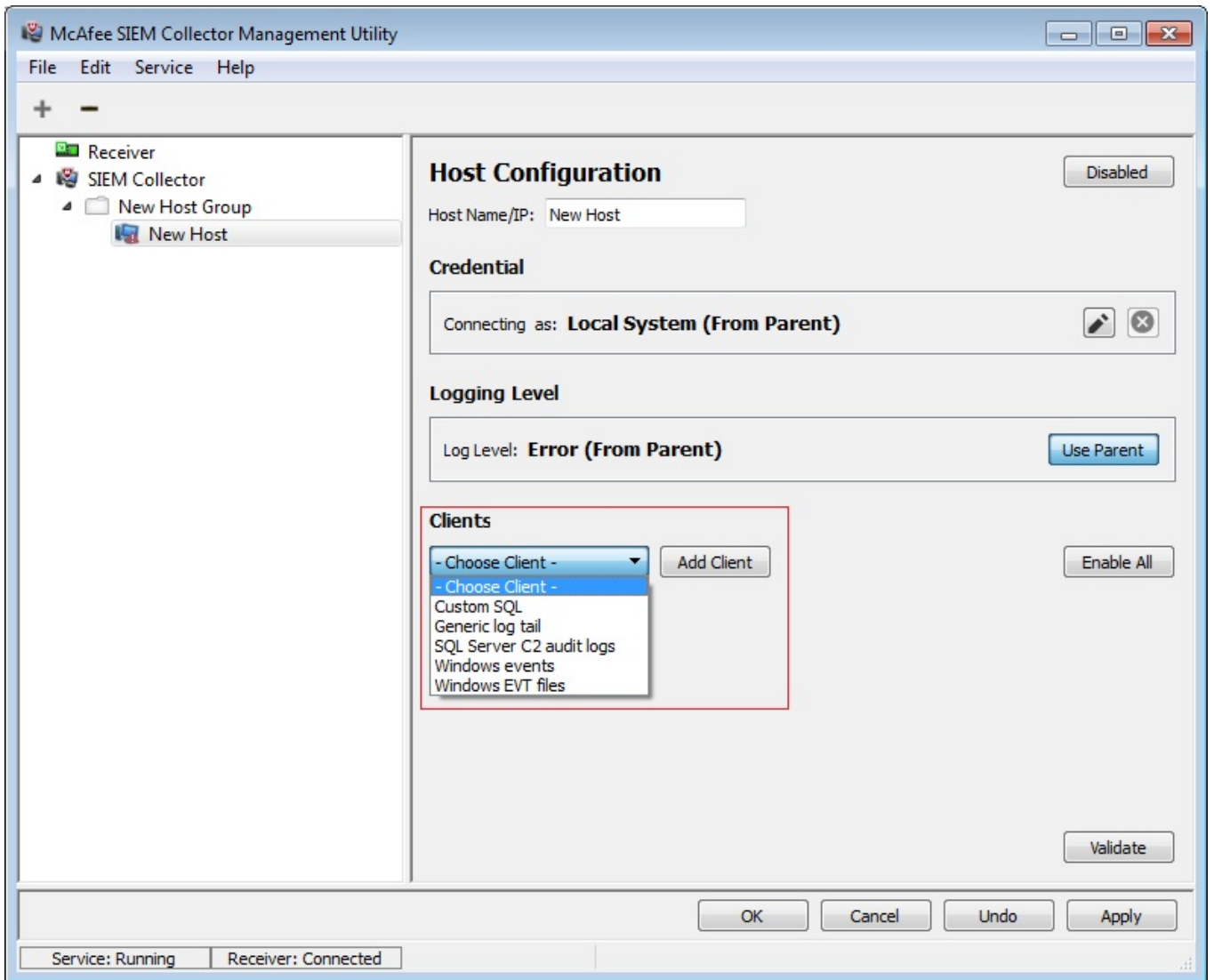
- On this screen you can change the name of your new host group and the credentials that will be used for collection . Click "Apply" to save changes.
- Credentials may be set at the Groups level and inherited by all child nodes in the group Individual nodes can be changed to not use the group's credentials 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 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.

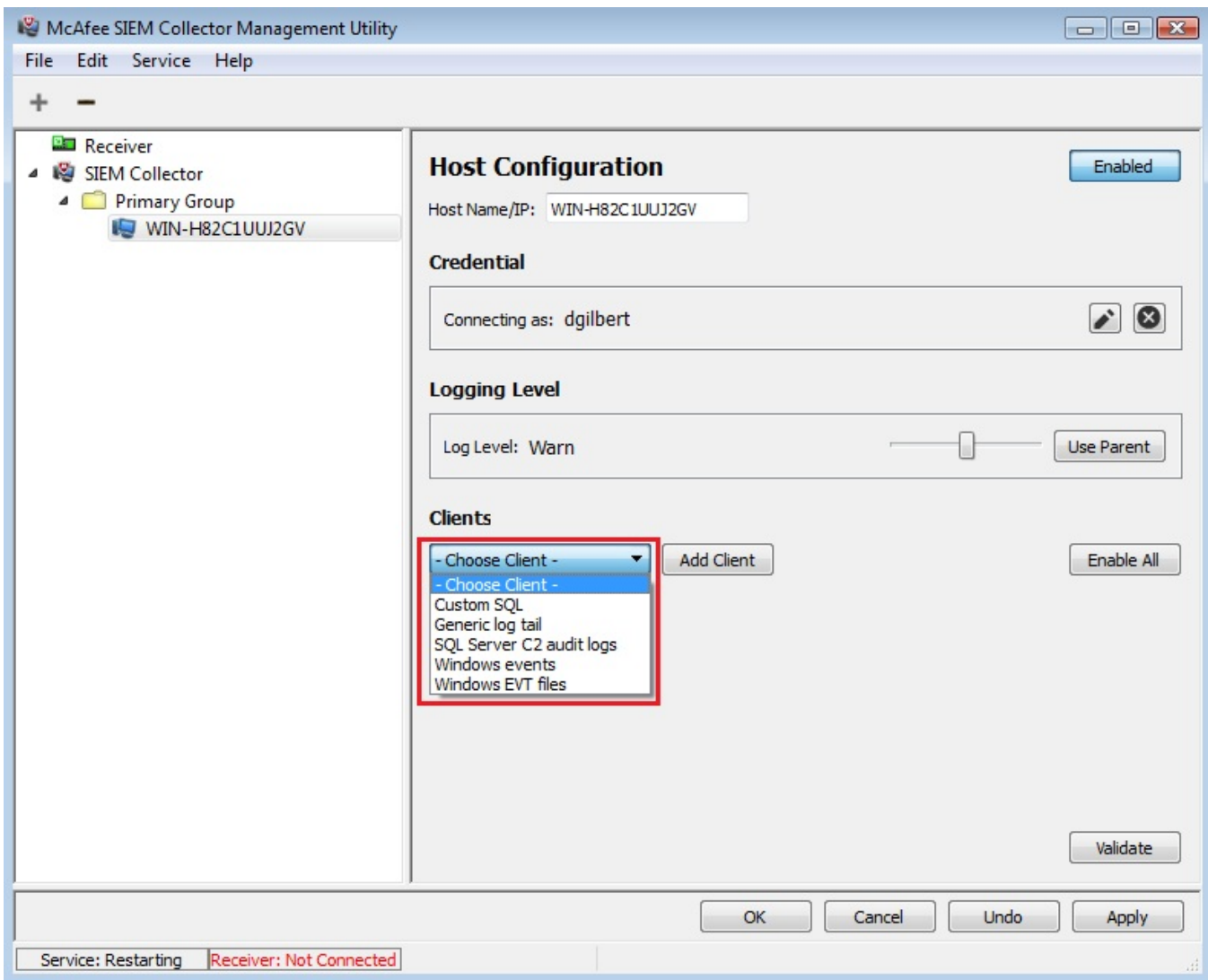
Note : Credentials are only validated when the host has enabled clients. Failed validation will disable the client/host.

- 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

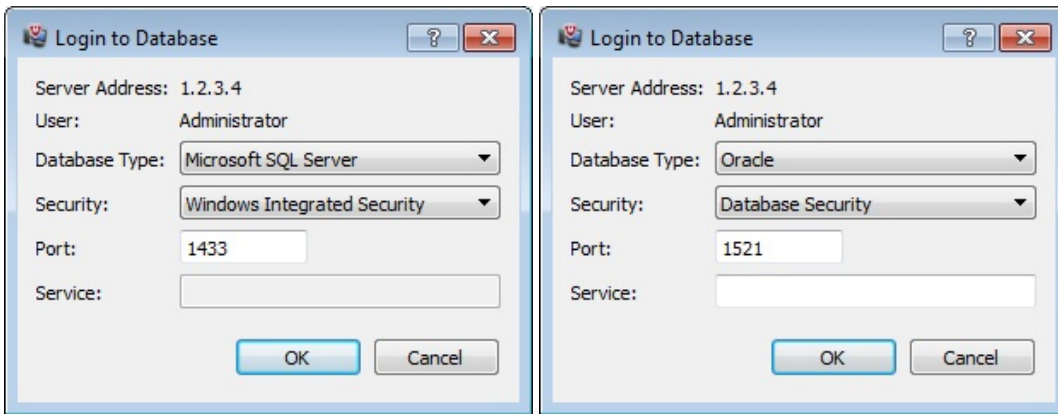
Oracle

- Download the Instant Client Package - Basic version 11.2.x.x
- Create a folder under C: called instantclient 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. The path recorded in the environment variable needs to point to the Oracle directory that contains the "vc9" directory.

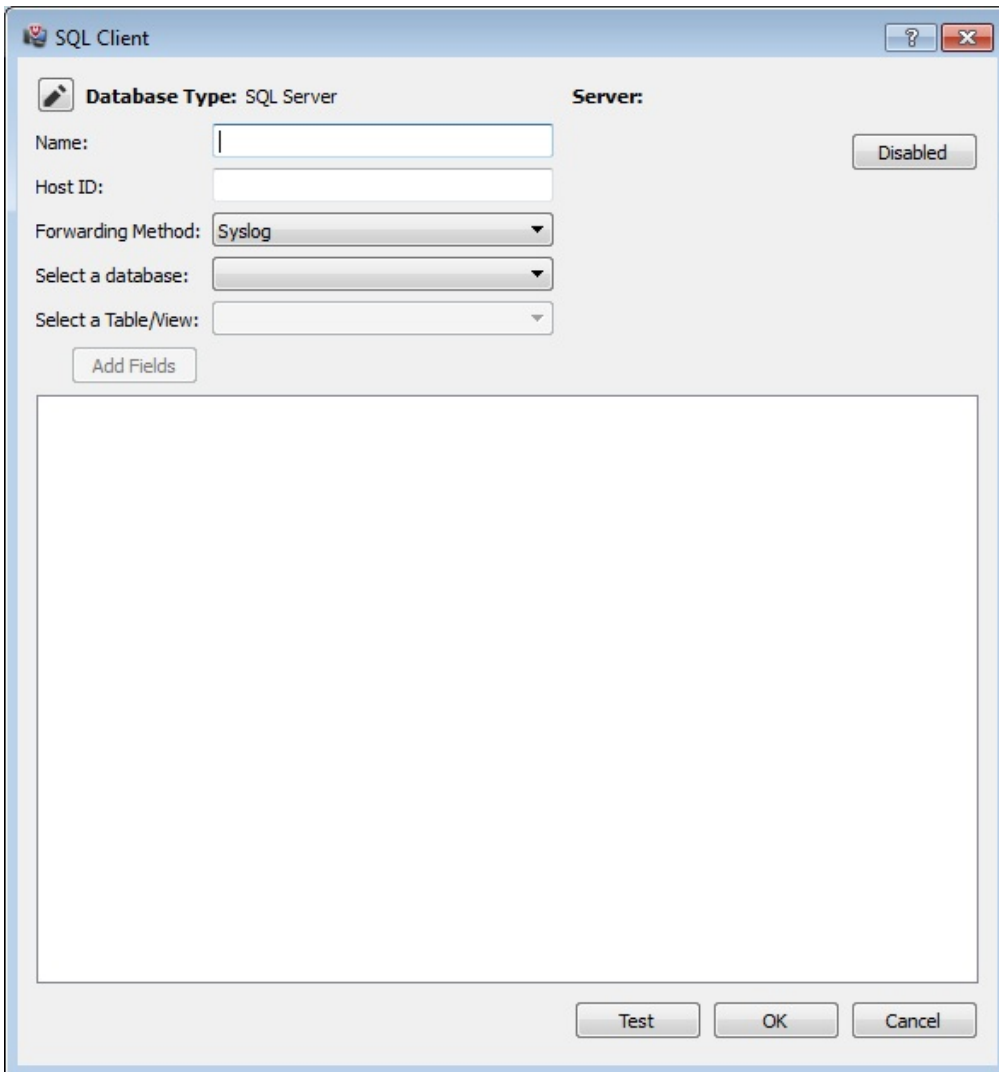
MSSQL

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.

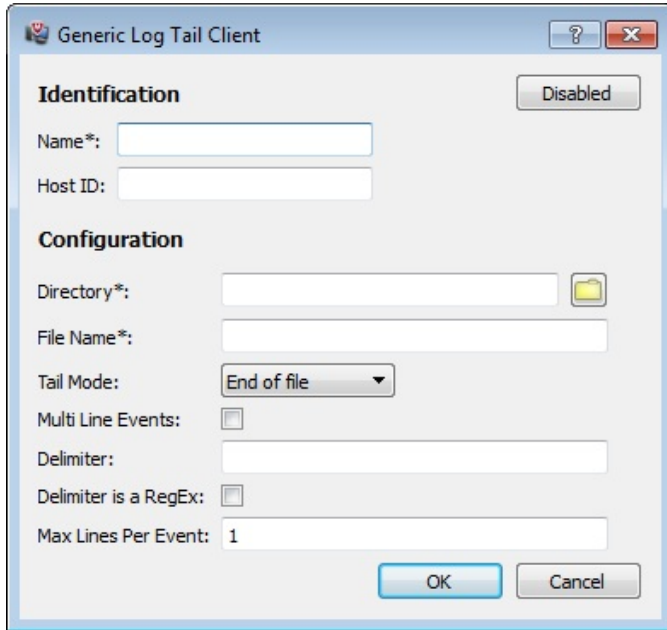
After configuring the login details, the "SQL Client" window appears. On this screen, the following fields can be configured:

- Name - *Required*. The name of the client.
- Host ID - An ID that corresponds to a host ID associated with a datasource 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.

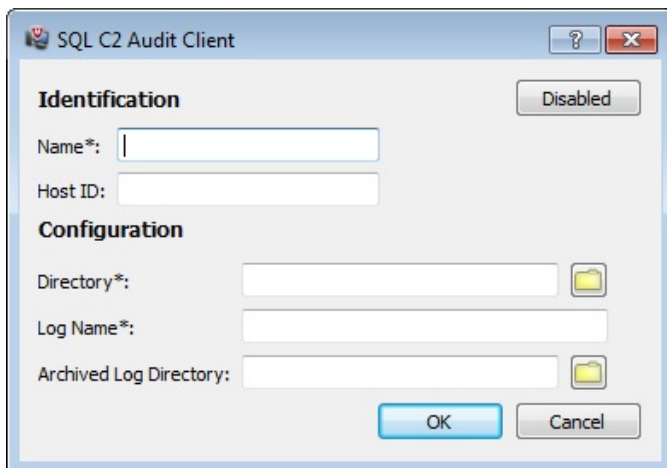
Generic Log Tail



The screenshot shows the 'Generic Log Tail Client' window. It has a title bar with a question mark and a close button. The window is divided into two sections: 'Identification' and 'Configuration'. In the 'Identification' section, there is a 'Name*' text box, a 'Host ID' text box, and a 'Disabled' button. In the 'Configuration' section, there is a 'Directory*' text box with a folder icon, a 'File Name*' text box, a 'Tail Mode' dropdown menu set to 'End of file', a 'Multi Line Events' checkbox (unchecked), a 'Delimiter' text box, a 'Delimiter is a RegEx' checkbox (unchecked), and a 'Max Lines Per Event' text box with the value '1'. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 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.
- 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}\V){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.

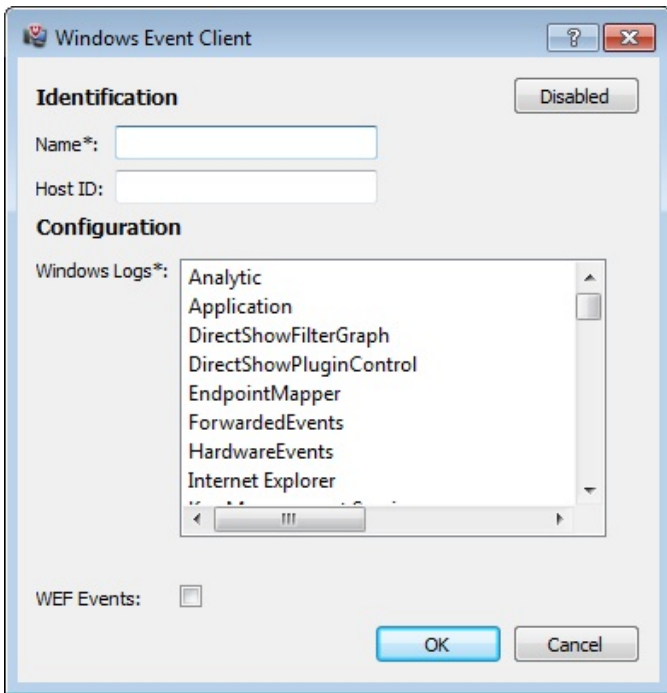
SQL Server C2 Audit Logs



The screenshot shows the 'SQL C2 Audit Client' window. It has a title bar with a question mark and a close button. The window is divided into two sections: 'Identification' and 'Configuration'. In the 'Identification' section, there is a 'Name*' text box, a 'Host ID' text box, and a 'Disabled' button. In the 'Configuration' section, there is a 'Directory*' text box with a folder icon, a 'Log Name*' text box, and an 'Archived Log Directory' text box with a folder icon. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 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.

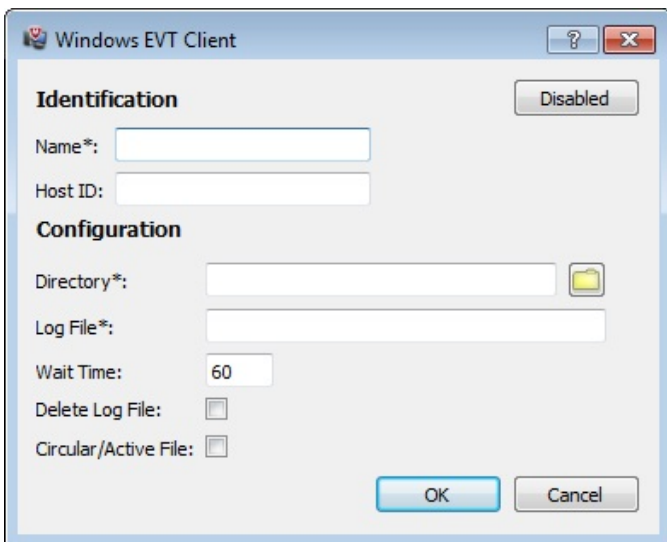
Windows Events



- Name - *Required*. The name of the client.
- Host ID - An ID that corresponds to a host ID associated with a datasource on the Receiver.
- Windows Logs - *Required*. A list of available logs on the machine. One or more must be selected to collect from.
- WEF Events - If checked, this indicates that the events are being forwarded from a remote machine and changes the "From" location to the hostname of the machine that generated the event. If unchecked, all events will show up on the Receiver showing a "From" location with the IP address of the machine that transmitted the events to the Receiver. In most (if not all) cases this is used with the "Forwarded Events" log.

Note: WEF events requires Windows Event Forwarding to be enabled between the Windows machines.

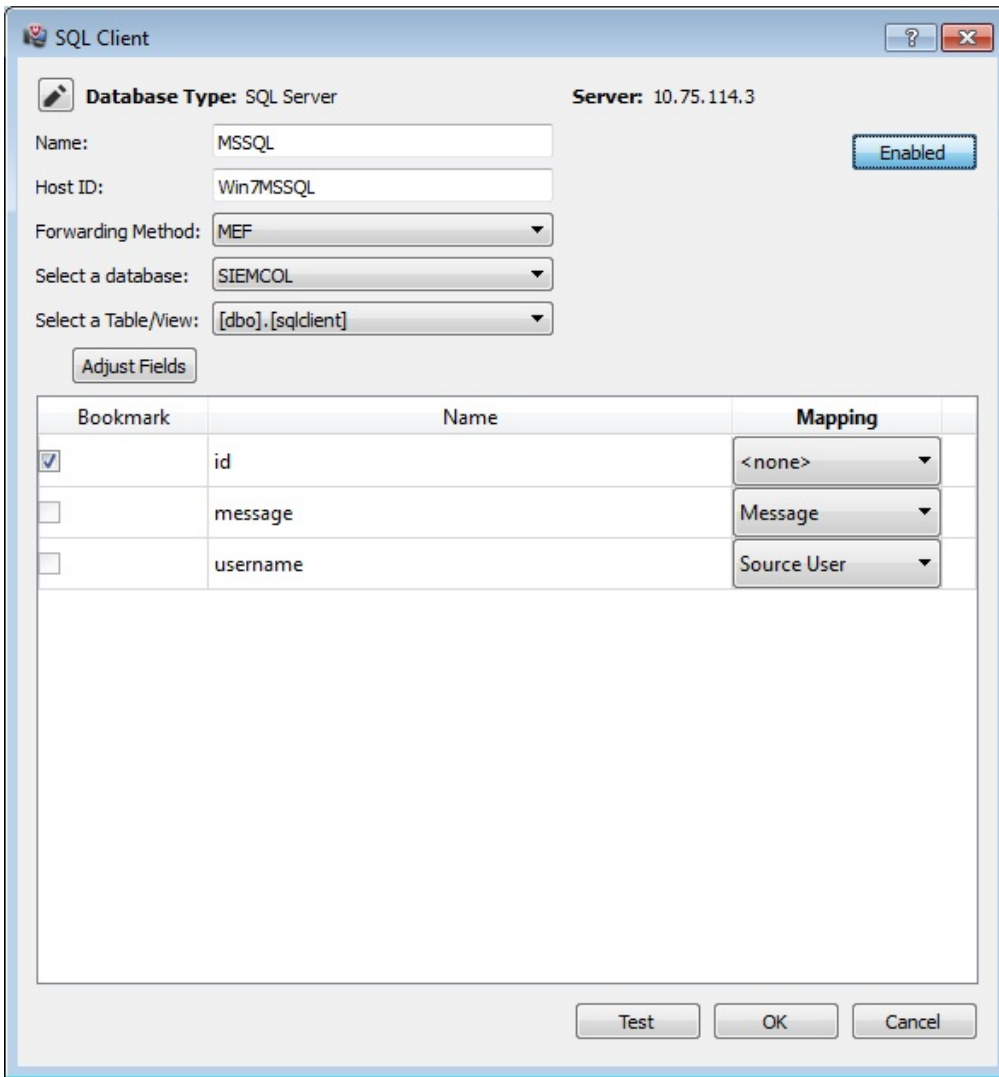
Windows EVT Files



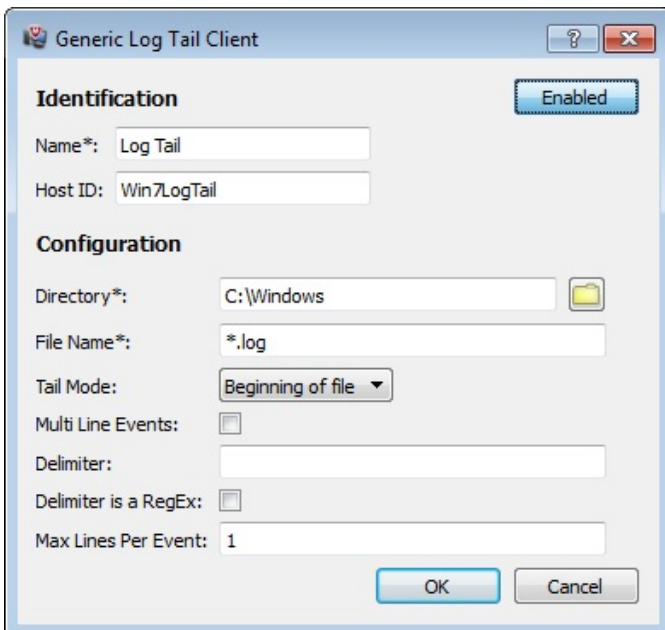
- Name - *Required*. The name of the client.
- Host ID - An ID that corresponds to a host ID associated with a datasource on the Receiver.
- Directory - *Required*. The path that the client will pull log files from. The directory field can be entered manually, or the file browser can be used to navigate to a path by clicking on the folder icon.
- Log File - *Required*. The name of the file that the client will read. This can be a full file name (i.e. "security.evtx"), or use wildcards (i.e. "*.evt" or "*.evt*").
- Wait Time - The minimum time to wait between reading log files.
- Delete Log File - If checked, the client will delete the log files after reading them.
- Circular/Active File - Indicates whether or not the log files are actively being written to by some other application or process.

Sample Windows Client Configurations

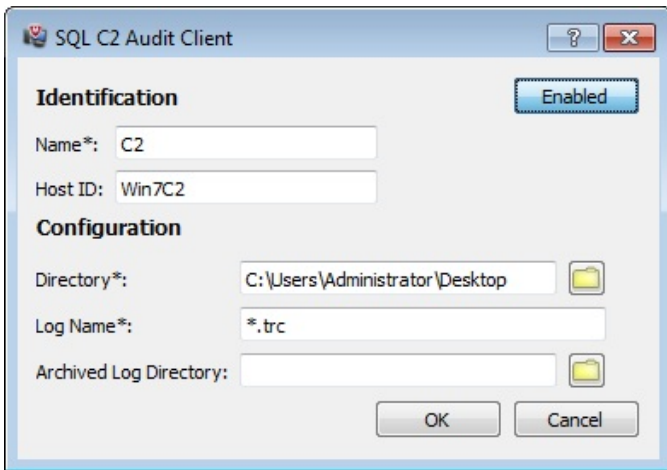
Custom SQL



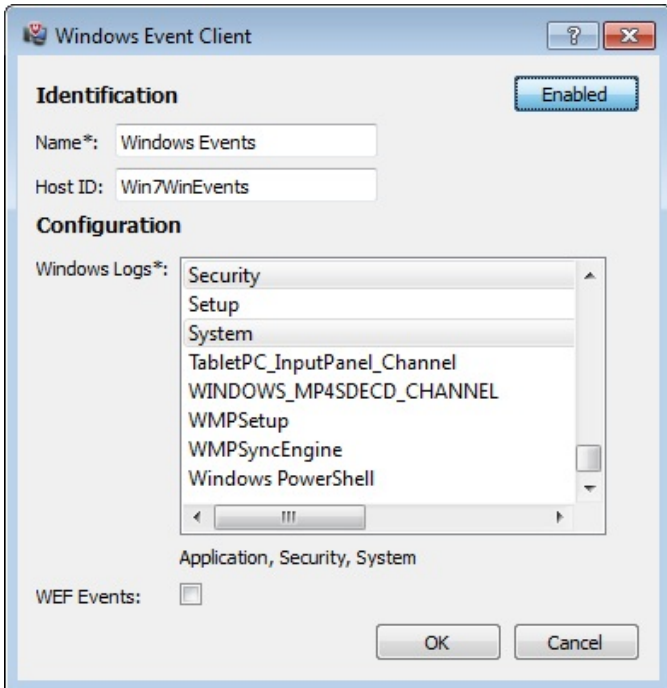
Generic Log Tail



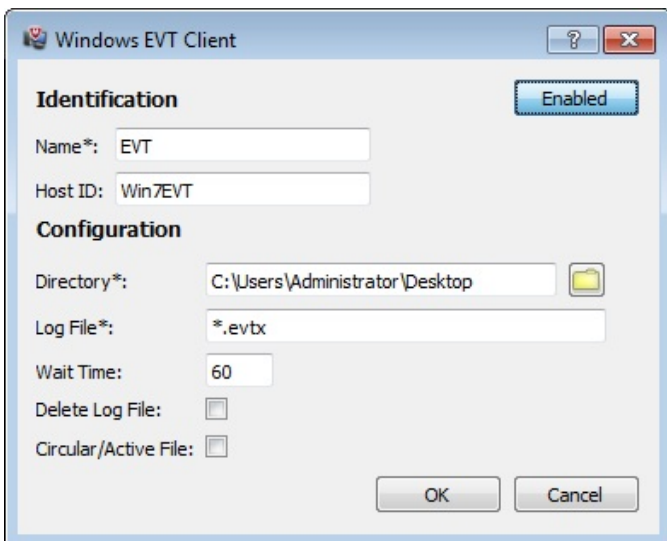
SQL Server C2 Audit Logs



Windows Events



Windows EVT Files



ESM DATA SOURCE CONFIGURATION

The ESM Datasource 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 Datasource for the IP Address that the SIEM Collector is transmitting from, or use the DHCP mask and host IDs.

Note : If a Host ID is used on the SIEM Collector then the ESM datasource may use the Host ID instead of an IP Address. Host IDs are case sensitive. (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 Datasource.

The screenshot shows the 'Edit Data Source' dialog for a Custom SQL data source. The 'Data Source Vendor' is set to 'Generic', 'Data Source Model' is 'McAfee Event Format', and 'Data Retrieval' is 'McAfee Event Format (Default)'. The 'Enabled' section has 'Parsing' checked, 'Logging' and 'SNMP Trap' unchecked. The 'Default Rule Assignment' is 'User Defined 1'. There are buttons for 'Interface', 'Advanced', 'OK', and 'Cancel'.

Use System Profiles:	No Profiles Defined
Data Source Vendor:	Generic
Data Source Model:	McAfee Event Format
Data Format:	Default
Data Retrieval:	McAfee Event Format (Default)
Enabled:	<input checked="" type="checkbox"/> Parsing <input type="checkbox"/> Logging <input type="checkbox"/> SNMP Trap
Name:	
IP Address:	
Host ID:	
Use encryption:	<input type="checkbox"/>
Default Rule Assignment:	User Defined 1

Generic Log Tail

The screenshot shows the 'Edit Data Source' dialog for a Generic Log Tail data source. The 'Data Source Vendor' is 'Generic', 'Data Source Model' is 'Advanced Syslog Parser', and 'Data Retrieval' is 'MEF'. The 'Enabled' section has 'Parsing' checked, 'Logging' and 'SNMP Trap' unchecked. The 'Time Zone' is '(GMT,00:00) Greenwich Mean Time', 'Support Generic Syslogs' is 'Do nothing', and 'Encoding' is 'None'. There are buttons for 'Interface', 'Advanced', 'OK', and 'Cancel'.

Use System Profiles:	No Profiles Defined
Data Source Vendor:	Generic
Data Source Model:	Advanced Syslog Parser
Data Format:	Default
Data Retrieval:	MEF
Enabled:	<input checked="" type="checkbox"/> Parsing <input type="checkbox"/> Logging <input type="checkbox"/> SNMP Trap
Name:	
IP Address:	
Host ID:	
Use encryption:	<input type="checkbox"/>
Time Zone:	(GMT,00:00) Greenwich Mean Time
Support Generic Syslogs:	Do nothing
Generic Rule Assignment:	User Defined 1
Encoding:	None

SQL Server C2 Audit Logs

Edit Data Source

Use System Profiles: No Profiles Defined

Data Source Vendor: **Microsoft**

Data Source Model: **MSSQL Server C2 Audit**

Data Format: Default

Data Retrieval: **MEF**

Enabled: Parsing **Logging** **SNMP Trap**

Name:

IP Address:

Host ID:

Use encryption:

Time Zone:

Interface Manage the network interface for the parent Receiver.

Advanced

Windows Events

Edit Data Source

Use System Profiles: No Profiles Defined

Data Source Vendor: **Microsoft**

Data Source Model: **Windows Event Log - WMI**

Data Format: Default

Data Retrieval: **MEF**

Enabled: Parsing **Logging** **SNMP Trap**

Name:

IP Address:

Host ID:

Use encryption:

Interface Manage the network interface for the parent Receiver.

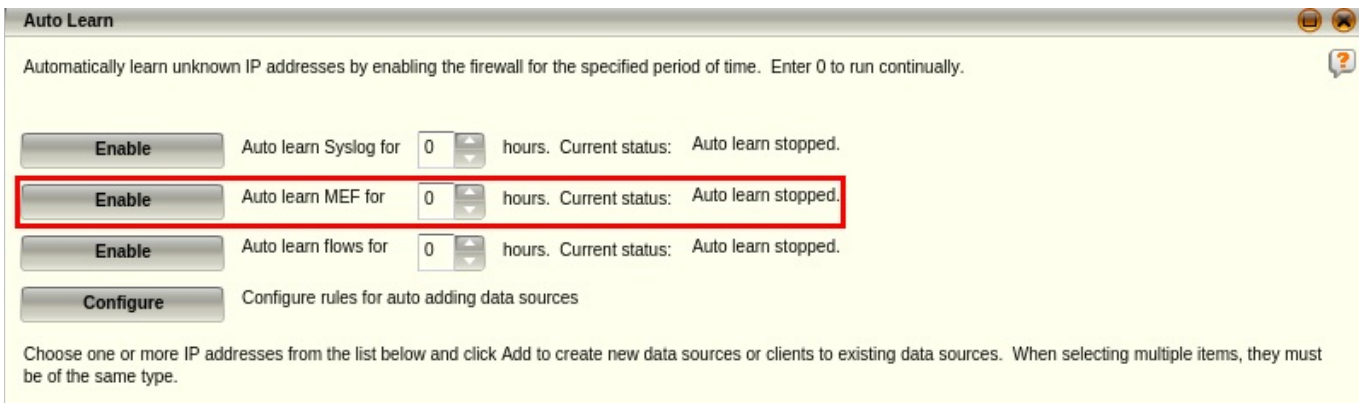
Advanced

Windows EVT Files

- The Windows EVT Files client is setup the same as the Windows Events.

AutoLearn

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



CONFIGURATION FILE

The SIEM Collector generates a configuration file (config.xml) when the application is installed using the Windows installer. The main purpose of this file is to tell the Collector how and where data should be parsed. It also can be used to perform a remote installation by being passed as an argument to msiexec. The configuration file is updated as changes are made within the Utility. The structure of the configuration file should look something similar to this:

```

1 <EventCollectorConfig LogLevel="Error" MaxLogSize="20971520">
2   <Credentials CredentialType="OtherAccount" Authenticated="true"/>
3   <Receiver IPAddress="10.75.84.153" Port="8082" Encrypt="false" AdapterIPAd
4   dress="10.75.84.40"/>
5   <HostGroup Name="Primary Group" Enabled="true" UseParentLogging="true">
6     <Credentials CredentialType="ParentSettings" Authenticated="true"/>
7     <Host Enabled="true" LocalHost="true" Host="WIN-H82C1UUJ2GV" IsHostVa
8   lid="true" UseParentLogging="true">
9       <Credentials CredentialType="ParentSettings" Authenticated="true"
10      />
11   />
12   <Client Enabled="true" IsClientValid="true" Name="Windows Applica
13   tion" ID="{1fcce90c-fe7c-4d53-95d1-7dc249891de5}" PluginType="WindowsEvent" C
14   lientType="WinEvent">
        <Configuration Key="Logs" Value="Application"/>
        <Configuration Key="useWEF" Value="0"/>
      </Client>
    </Host>
  </HostGroup>
</EventCollectorConfig>

```

This configuration file can also be used to perform a remote installation of the SIEM Collector. Note that when using the configuration file to install the SIEM Collector remotely, it does not need a .xml extension. The important thing is that the contents of the file are valid XML. However on the Windows machine itself the Utility will specifically look for a config.xml file to load. It is possible to modify the XML manually instead of using the Utility. Here is a list describing the XML nodes that the SIEM Collector uses for reference:

- < EventCollectorConfig > - The root XML node.
 - LogLevel - Possible Values:
 - Error - Logs errors
 - Info - Same as Error but also logs related information
 - Warn - Same as Info but also logs warnings
 - Debug - Same as Warn but also logs debug information
 - Diagnostic - Same as Debug but also logs diagnostic information
 - MaxLogSize - The maximum size in bytes of the log file. When the maximum size is reached, the new information will write over the oldest information. The debug file is called debug.log and is stored in the directory where the Collector was installed
- < Credentials/ > -
 - CredentialType - Possible values: OtherAccount, ParentSettings
 - Authenticated - Possible values: true, false
- < Receiver/ > -
 - IPAddress - The IPAddress of the target Receiver
 - Port - The MEF port used by the target Receiver
 - Encrypt - Encrypt data sent to the Receiver. Possible values: true, false
 - AdapterIPAddress - IP of the network adapter being used
- < HostGroup > -
 - Name - Name of the group
 - Enabled - Enable/Disable all hosts in the group. Possible values: true, false
 - UseParentLogging - Use credentials of the SIEM Collector node. Possible values: true, false
- < Credentials/ > -
 - CredentialType - Possible values: OtherAccount, ParentSettings
 - Authenticated - Possible values: true, false
 - Username - Username of the Windows machine
 - Password - Password of the Windows machine
- < Host > -
 - Enabled - Enable/Disable all hosts in the group. Possible values: true, false
 - LocalHost - Using local machine or not. Possible values: true, false
 - Host - The hostname/IP Address of the windows machine.
 - IsHostValid - Used by the Utility to show if the hosts are valid or not. Possible values: true, false

- UseParentLogging - Use credentials of the host node. Possible values: true, false
- < Client >
 - Enabled - Enable/Disable the host. Possible values: true, false
 - IsClientValid - Did the client successfully connect? Possible values: true, false
 - Name - Name of the client
 - ID - Unique ID generated by Utility
 - PluginType - Possible Values: WindowsEvent, MEF, Syslog
 - ClientType - Possible Values: WinEvent, WinEVT, C2Audit, LogTail
- < Configuration/ > - Client specific configurations
 - Key - Maps to the Value for a configuration

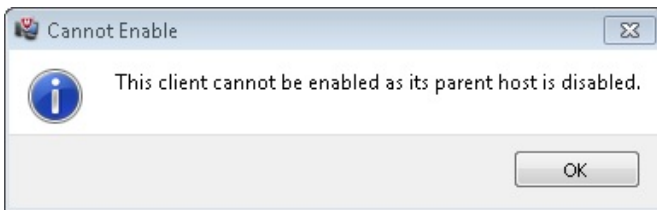
TROUBLESHOOTING

SIEM Collector Utility

Does not boot and fails silently

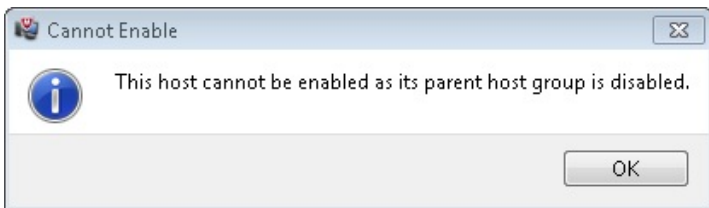
If the XML of the config.xml file is not formatted properly the Utility will not load and will not display any error messages. Check the XML and make sure all tags are closed properly.

Cannot Enable Client



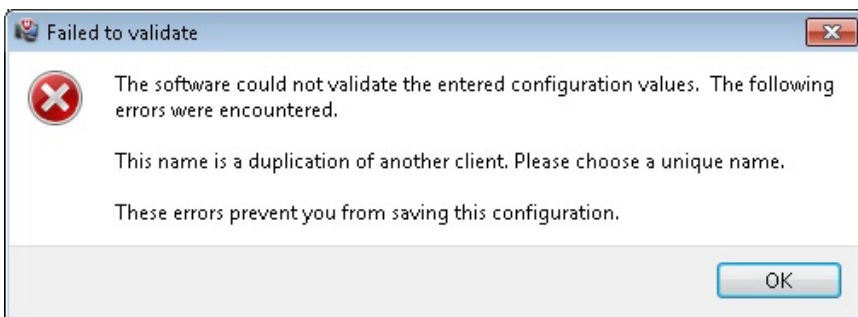
1. You will need to enable the parent group.
2. You will need to enable the parent host.

Cannot Enable Host



1. You will need to enable the parent group.

Cannot Enable Client



- Verify you have the correct host/ip.
- Verify that the host/ip you are connecting to is powered on.
- Verify that the username/password for this host/ip used is correctly.
- Verify that the host/ip you are connecting to can get through the firewall.
- Verify the host/ip is not behind a proxy.