Boldon James
A QINETIQ company

Classifier Reporting System Guide

UM642309

February 2020

Gold Microsoft Partner

Microsoft

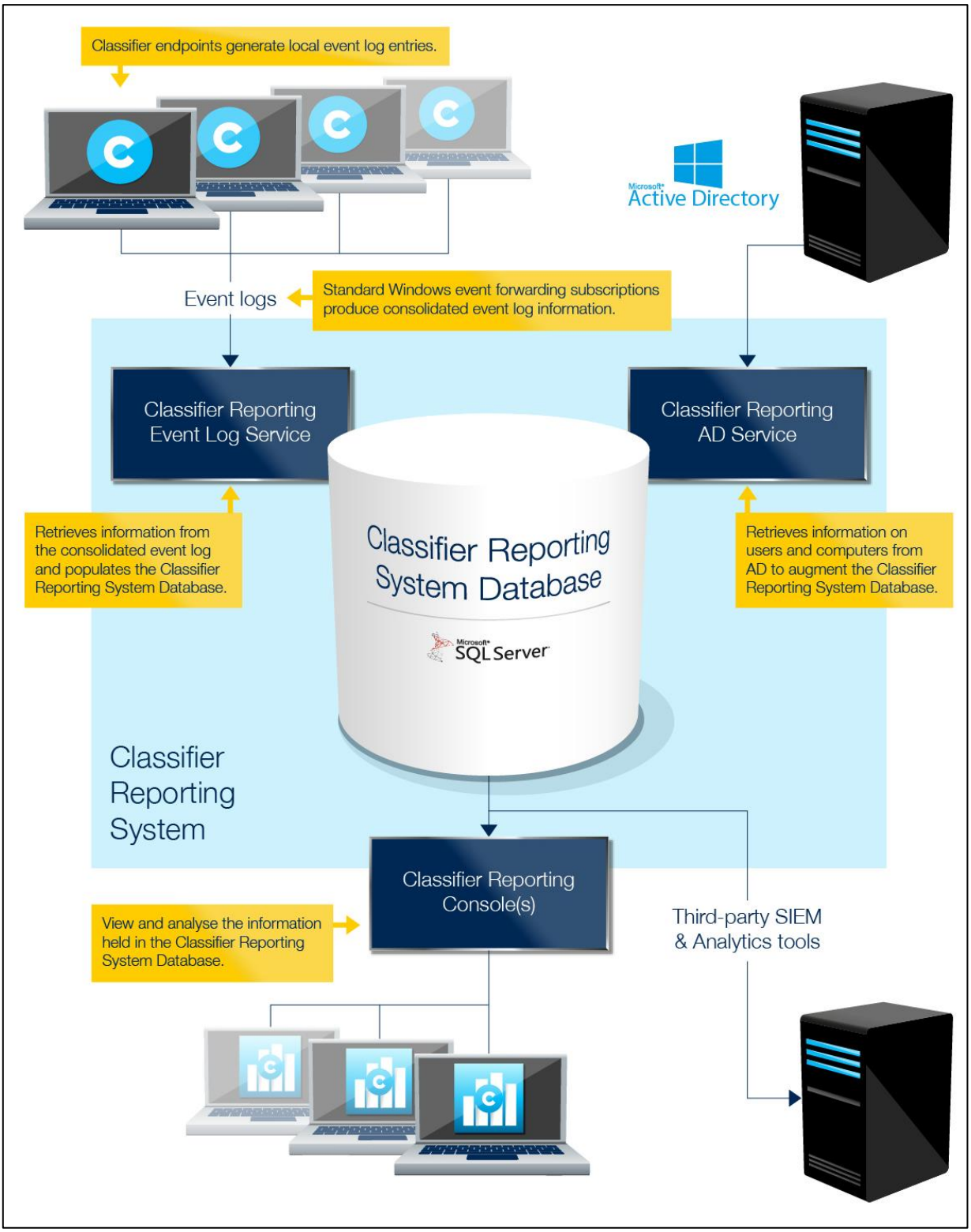
Customer Documentation

Contents

1 INTRODUCTION

This is the Classifier Reporting Services Guide for **version 1.4.1** of the Classifier Reporting Services.

Boldon James **Classifier Reporting Services** delivers dashboards and reports that provide administrators and managers insight into the way that Classifier components are being used in their organisations. The **Reporting Services Components** diagram below shows the structural relationship between the components supplied and other system components.



Reporting Services Components

Classifier Reporting Services comprises the following components:

- **Classifier Reporting Services**, which includes the following features all described in this document:
  - **Classifier Event Log Service**

This periodically retrieves Windows Classifier application (e.g. Office Classifier and Email Classifier) event log information from the Consolidated Event Log server and populates the Classifier Reporting Database.

The Consolidated Event Log is produced using standard Windows mechanisms as described in the section on Classifier Event Forwarding.

This feature also installs the **Configuration Wizard** that allows the AD and Event Service to be configured and encrypts the SQL connection details when using SQL Server Authentication.

- **Database Management**

  This component is used to establish the Classifier Reporting Database on a SQL Server. [This component also provides a **DataCreator** program which provides the ability to populate the Classifier Reporting Database with example data as described in the **Classifier Reporting Starter Guide (UM6438)**.

- **Classifier AD Service**

  This periodically retrieves information on users and computers from Active Directory and populates the Classifier Reporting Database. The Classifier AD Service is not installed by default and should only be installed if you wish to retrieve user and computers information and use the information in reports.

  This feature also installs the **Configuration Wizard** that allows the AD and Event Service to be configured and encrypts the SQL connection details when using SQL Server Authentication.

- **Channel Wizard**

  This component can be used to create event log channels that are needed to forward events to the Consolidated Event Log server.

- **Migration Wizard**

  This component can be used to migrate the data from a V1.1 database to a V1.2 database.

- **Support Libraries**

  These libraries are common to all features and will always be installed.

- **Classifier Reporting Console**

  This component provides the dashboards and reporting interface which uses the information stored in the Classifier Reporting Database. Further information can be found in the **Classifier Reporting Console Guide (UM6422)**.

As shown above third party tools such as Security Information and Event Management (SIEM) tools can extract and analyse the data. The accompanying **Classifier Reporting Console Guide (UM6422)** specifies the database in some detail so that third party tools can examine the data.

The Event Log Service should be installed on the Consolidated Event Log server. The AD Service can be installed on the same system as the SQL Server or a separate system.

To establish a working Classifier Reporting Services system:

1. Decide on your deployment structure (which services are to be installed on which system).
2. Ensure SQL server is installed and operational.

3. Familiarise yourself with the system requirements and Classifier Reporting Services installation process in section 2.
4. Install the **Classifier Event Log Service**, the **Database Management** component and optionally the **Classifier AD Service** and **Channel Wizard**
5. Establish the necessary event forwarding to the Consolidated Event Log server as described in the section on Classifier Event Forwarding.
6. Create the Classifier Reporting Database with the installed **Database Management** component as described in the section The Classifier Reporting Database.
7. Configure the **Event Log Service** as described in the section Configuring the Event Log Service.
8. Configure the **AD Service** as described in the section Configuring the AD service.
9. Install **Classifier Reporting Console** as described in the accompanying **Classifier Reporting Console Guide (UM6422)**.

2 INSTALLATION AND SYSTEM REQUIREMENTS

The following section lists the requirements of computers used in the Classifier Reporting Services.

2.1 Classifier Clients

All computers running Classifier products should meet the following requirements:

1. Users should have Active Directory user accounts joined to the local Active Directory domain.
2. The Windows program **Winrm** must be available if using Windows Event Forwarding described in Collector initiated event forwarding; Winrm is available out of the box on Vista or later operating systems. See http://windowsitpro.com/security/q-what-windows-platforms-support-windows-event-forwarding-and-collection for full details.

2.2 Classifier Configuration

The Event Log Service must have access to a published Classifier Configuration so that it can access definitions of labels and policies needed to parse Event labels into individual selector values. Parsing labels into individual selector values enable users of the **Classifier Reporting Console** to drill-down into labels on dashboards.

The label marking format used for Event labels is defined in the Classifier configuration by the Custom format for 'Classifier Auditing' setting – see Classifier Administration Guide > General Settings for more details. To improve the parsing of individual selector values, the marking prefix and suffix of selector elements in the marking format, should not be a space character.

Classifier configurations can be published to either a local file store or to an Active Directory. The Event Log Service uses the same mechanisms as other Classifier components to access the configuration as defined by registry keys that must be established before the Event Log Service is run. Use of **Service Mode** entries is recommended - see Classifier Administration Guide > Configuration Deployment and Classifier Administration Guide > Configuration Registry Search Algorithm for more details.

You must supply registry key values for LabelConfiguration, Policy, ServerFileSystemRoot (if using a fileshare) and ServerRootType. You must provide a policy name from your Classifier

configuration for the Policy key value. You may use any Classifier policy name from your configuration.

Note: The Classifier Reporting System does not support retrieving Classifier configuration information from web locations.

2.3 Installing Classifier Reporting Services

2.3.1 Before Installation

1. You are strongly advised to read this guide to gain an understanding of the product's components.
2. Administrator privileges are needed to install Classifier Reporting Services.
3. Microsoft .NET Framework 3.5 is not installed by some versions of Microsoft SQL Server and should be installed before the Classifier Reporting Services is installed on your system.
4. If you are upgrading from version 1.0.0 or version 1.1.0 and you wish to continue using the Classifier Reporting Database created by the earlier versions then it is recommended that you read the section entitled 'Upgrading the Classifier Reporting Database' before you uninstall the earlier version.
5. If you are upgrading from version 1.0 to version 1.2, please note that the Boldon James Management Agent event channel created by the version 1.0 Installation contained an incorrect name and should be removed before removing version 1.0 and installing version 1.2. Details are provided in the section entitled 'Forwarding Management Agent Events'.

2.3.2 Uninstalling a previous version

To un-install follow these steps:

1. Stop the Event Log service or the AD service if you have installed them.
2. Navigate to 'Control Panel' > 'Programs and Features'. The entry Boldon James Classifier Reporting Services appears in the list of installed programs. Select it and click 'un-install'. Confirm this operation when prompted and the product will be removed.
3. This will not remove the Classifier Reporting Database. The section Removing the Classifier Events Database contains details of how to remove the Classifier Reporting Database. Do not remove the Classifier Reporting Database if you want to upgrade to a later version of Classifier Reporting Services.
4. If during the uninstallation a warning is displayed stating that a set of applications should be closed before continuing, the 'Do not close application' option should be selected and the OK button pressed.

2.3.3 Installing

1. To install one or more of the components of Classifier Reporting Services complete the following steps:
2. If you are upgrading from an earlier version of the Classifier Reporting Services please remove the earlier version as explained in the section entitled Uninstalling a previous version.

3. Open the Classifier Reporting Services folder in the Classifier Reporting Services bundle and run **Classifier Reporting Service.exe**.
4. Select which components you wish to install.
5. If you choose to install either the AD Service or the Event Log Service, you will be prompted to define the Windows domain account that will run the services as shown below (see Configuring the Event Log Service for more details).

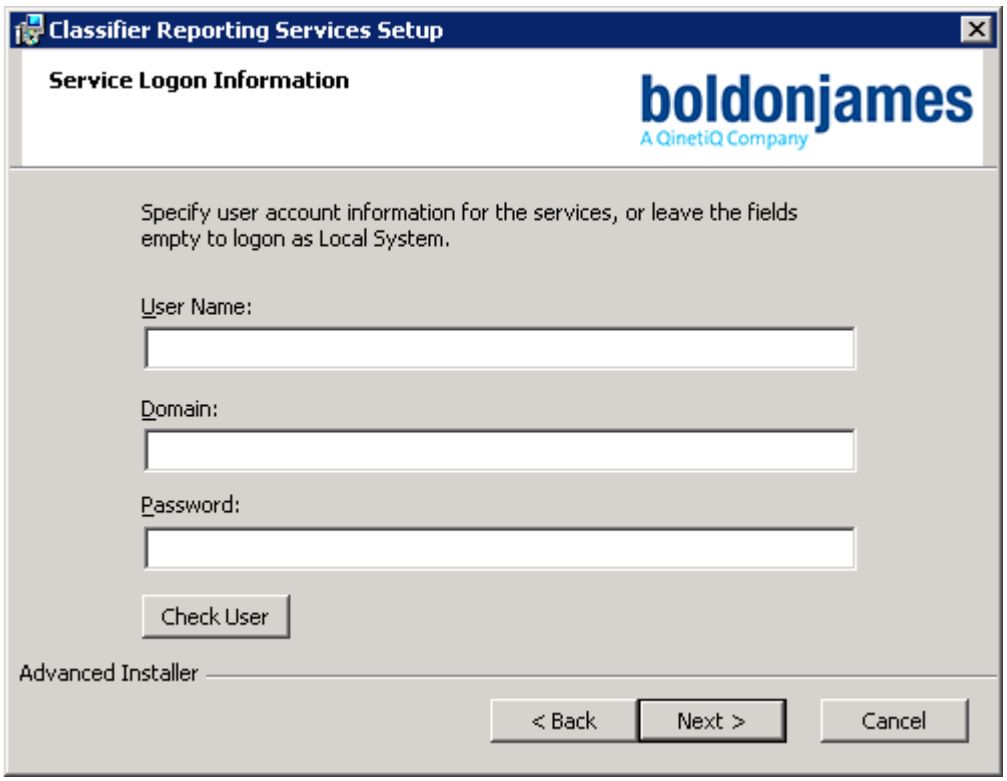


Figure 1 - Windows service logon information

If you enter any account details, the AD Service / Event Log Service being installed will be configured to run as that account.

Note: If you enter details of a non-existent account the installation may fail with an error stating that you have insufficient privileges to install the system services. If you have doubts about which account to use you should consider entering no account details and configure the services after installation.

If the account details are not filled in, the service(s) being installed will be configured to run as the Local System account.
The service(s) logon do not have to be configured during installation - see Configuring the Event Log Service and Configuring the AD Service for more details.

You will then be prompted to enter the SQL connection details as below:

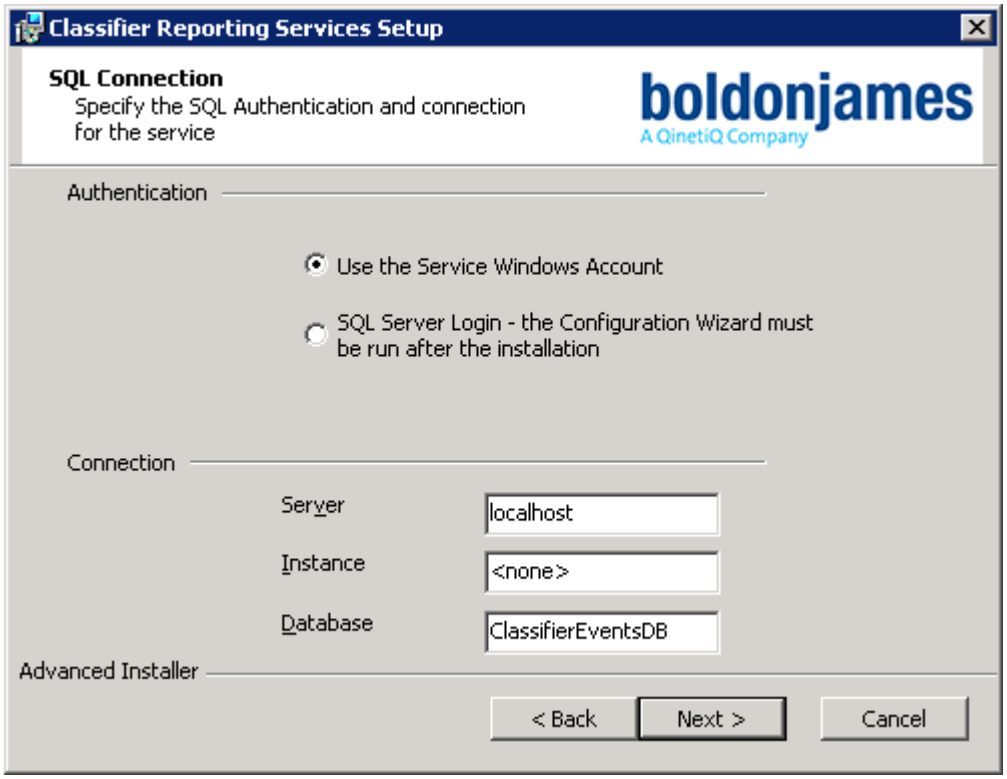


Figure 2 - SQL authentication and connection details

The service(s) SQL authentication and connection details do not have to be configured during installation - see Configuring the Event Log Service and Configuring the AD Service for more details.

6. The selected components will then be installed.
7. If you install one or more components, a **Classifier Reporting Services** menu item will be created under **Programs and Features**.

2.3.4 Licensing the Event Log Service

This version of the Event Log Service uses the same licensing mechanism as the other products in the Classifier family that is licences are applied and managed by the Classifier Administration tool. In particular to licence this product you will need a separate 'Classifier Reporting Service' licence.

The Classifier Administration Guide explains how to licence Classifier products, see Classifier Administration Guide > Settings applicable across the organisation->Global Settings->Licence for more details. If you are installing the Event Log Service for the first time you must follow these instructions to licence the product.

Note: If you are upgrading from an earlier version (V1.3.1 or earlier) you must re-licence the Event Log Service by using the Classifier Administration tool with a new Classifier Reporting Service (CRS) licence. It is not possible to re-licence the Event Log Service with the Classifier Reporting Tool (CRP) licence used to licence earlier version (V1.3.1 or earlier) of the Event Log Service.

3 CLASSIFIER EVENT FORWARDING

The purpose of event forwarding is to collect events from client computers running Classifier to an Event Log on a central server called the Consolidated Event Log server. Event forwarding can be configured to be either collector initiated (pull) or source initiated (push). This section describes two ways of configuring event forwarding:

- Collector initiated Event Forwarding
- Source initiated Event Forwarding using Group policy

The procedures described in this document use features of Microsoft Windows operating systems including Windows Remote Management (WinRM). The steps in the procedures should be carried out by a Domain Administrator and apply to WinRM version 2.0.

This section is just a brief introduction to event forwarding and contains a minimum set of steps. It does not explore situations such as forwarding events from computers outside of a domain. For more information on event forwarding see Configure Computers to Forward and Collect Events.

3.1 Collector initiated Event Forwarding

To configure collector initiated event forwarding, steps have to be taken on each Classifier client computer and the Consolidated Event Log server. These steps are discussed in the next two sections.

3.1.1 Classifier Clients

On each of the Classifier client computers from which you wish to collect events, the Windows Remote Management (WinRM) service has to be started and the firewall has to be configured to allow events to be forwarded, this is done by completing the following step.

1. In a Windows Command console, type:

   `winrm quickconfig`

   and answer “y” (yes) when prompted, as shown below.

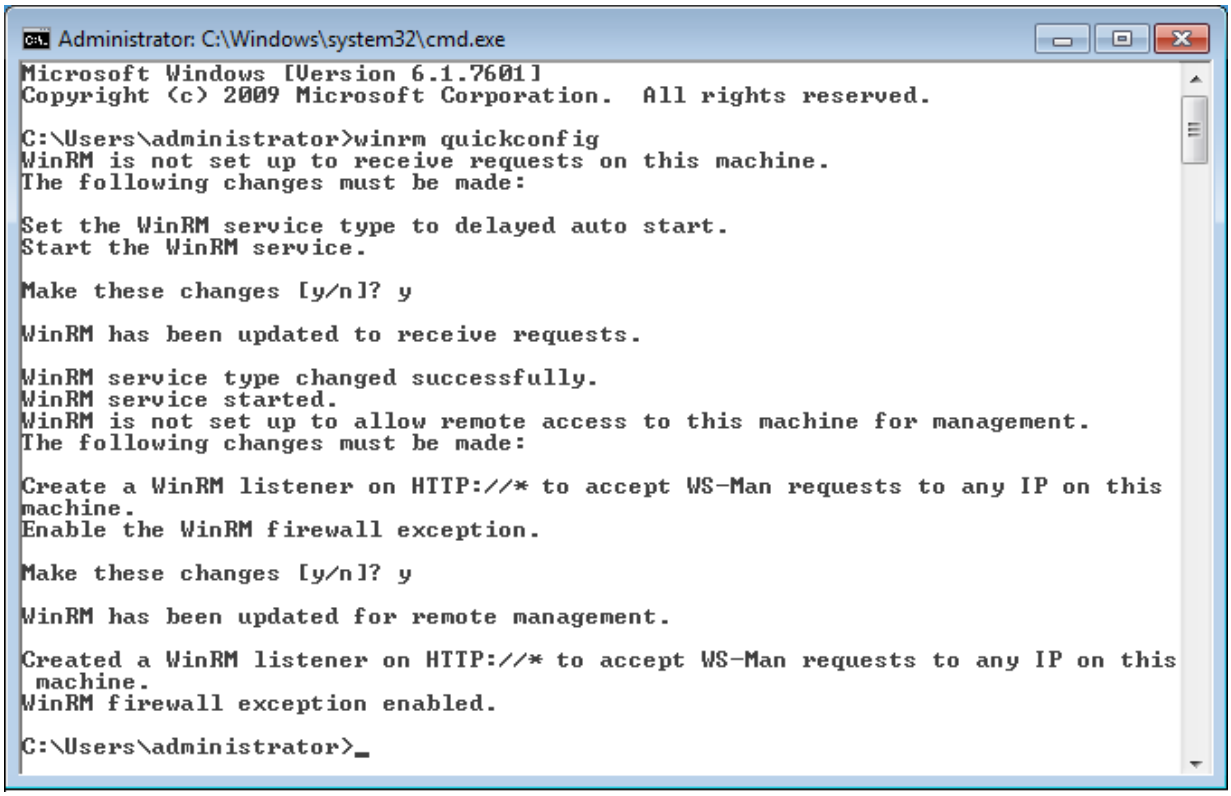


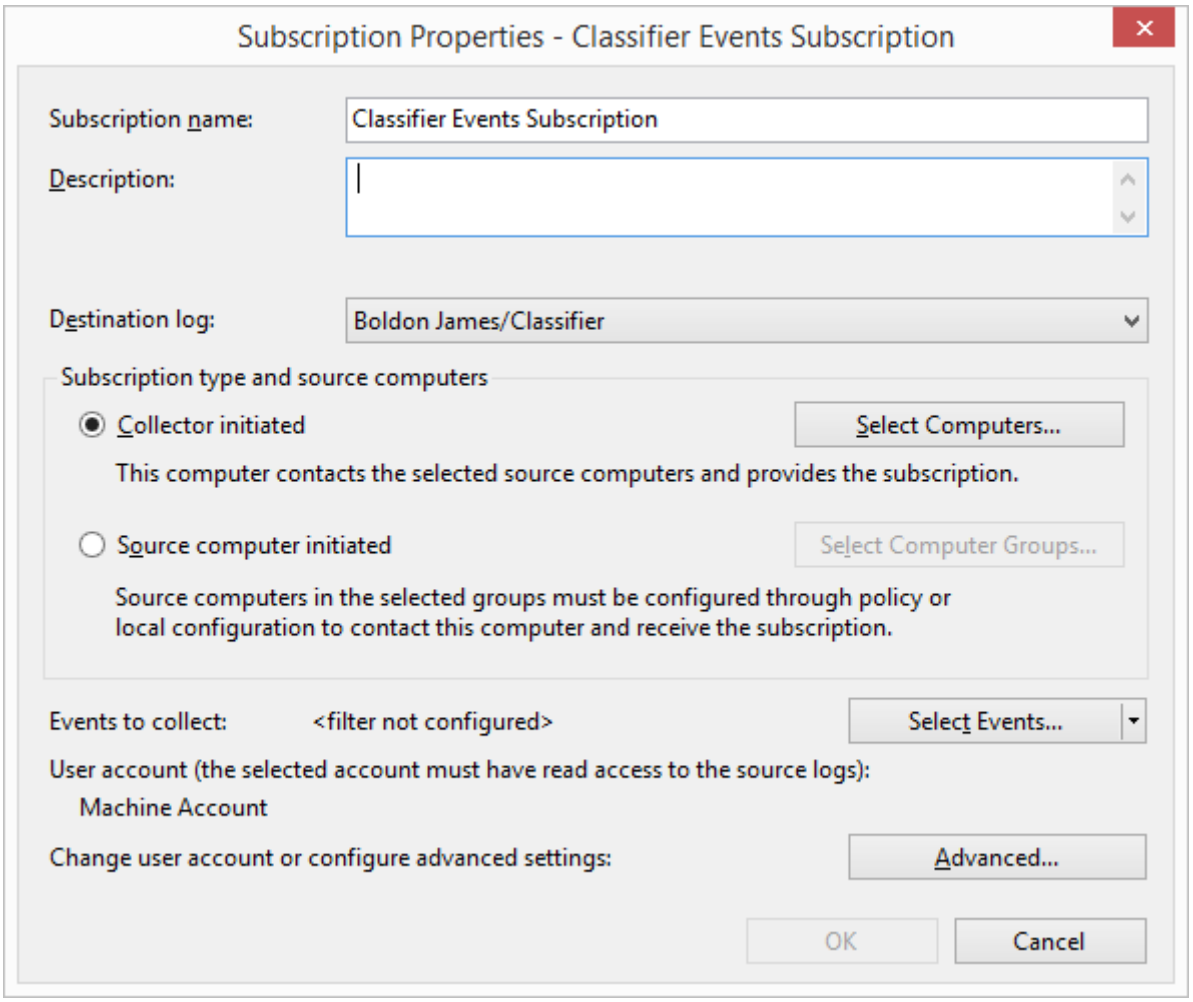
Figure 3 - WinRM command

3.1.2 Consolidate Event Log Servers

On the Consolidated Event Log server, a subscription should be defined to collect the events from the Classifier client computers. This section will explain how this can be done.

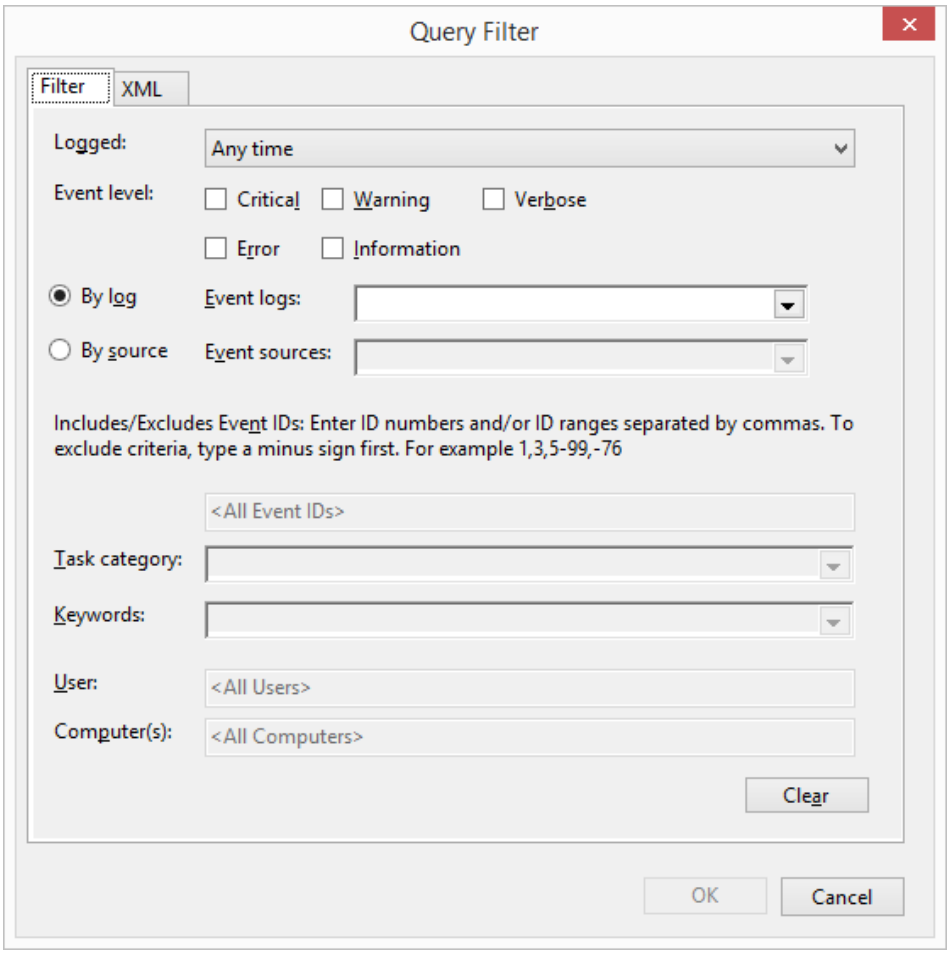
1. Start **Event Viewer**, select the **Subscriptions node** and choose "**Create Subscription…**" from the context menu. The **Subscription Properties** dialog will be displayed.

Note: If this is the first Subscription to be created you will be prompted that the Windows Event Collector Service must be running. Press Yes and the Services program will be displayed allowing you to start the service.



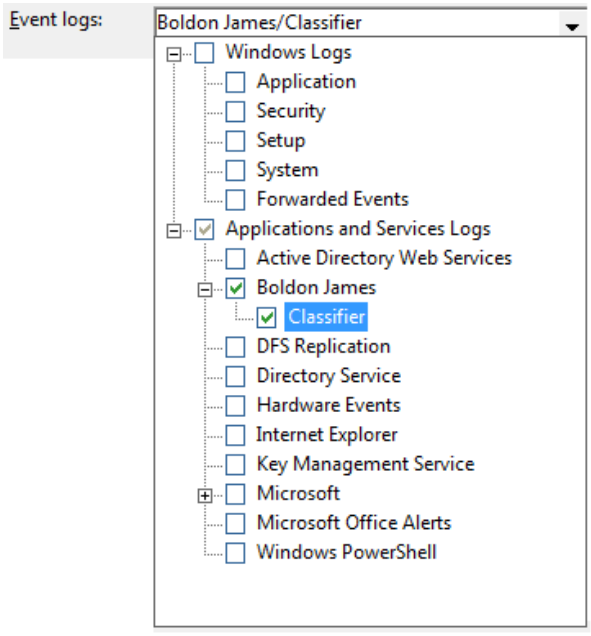
Create Events Subscription

2. Provide a name for the subscription, for example "**Classifier Events Subscription**".
3. Select the **Boldon James/Classifier** event channel from the **Destination log**: drop-down list. The **Boldon James/Classifier** event channel is created if you install the Event Log Service. Alternatively if you wish to collect events to a server without installing the service you can create the channel by running the Event Channel Wizard.
4. Select **Collector Initiated**.
5. Press **Select Computers…** and identify the computers that you wish to collect events from.
6. Press **Select Events…** and the **Query Filter** dialog is displayed



Event Subscription Filter

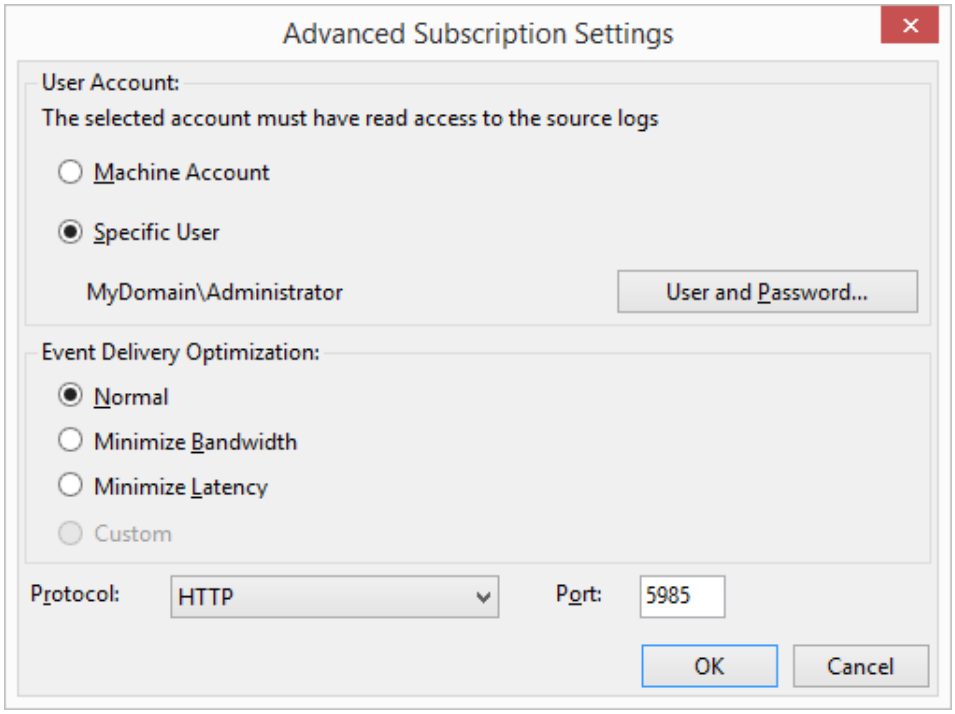
7. Select all of the **Event level** check boxes.
8. Select **By log** and then select **Boldon James/Classifier** Event Channel in the **Event Logs** dropdown as shown below.



Choose Event logs

9. Press **OK** to return to the **Subscription Properties** dialog.

10. Press **Advanced** and the **Advanced Subscription Settings** dialog is displayed



Advanced Subscription Settings

11. Set the **User Account** to the Domain Administrator e.g. ***MyDomain\Administrator*** by selecting **Specific User** and then pressing the **User and Password…** button.
12. Set **Protocol** to **HTTP**.
13. Press **OK** to return to the **Subscription Properties** dialog.
14. Press **OK** to complete the subscription.
15. The events collected by this subscription must be collected in **Event** format, not **RenderedText** format which is not usable by the Classifier Reporting database. To configure collecting in **Event** format run a Windows Command console and type

```
wecutil ss "Classifier Events Subscription" /CF:Events
```

Note “Classifier Events Subscription” is the name of the subscription created in step 2 above.

3.2 Source initiated Event Forwarding using Group Policy Objects

Source initiated event forwarding uses Active Directory Groups and Group Policy Objects (GPO) to configure Classifier client computers to forward events to the Consolidated Event Log server. This procedure consists of four steps

1. Create an Active Directory group containing all the Classifier client computers that are to forward events.
2. Define a GPO and apply it to the group created above.
3. Define a Classifier events subscription on the system that is to receive the forwarded events and link it with the group.

4. Re-start all the Classifier client computers in the group so that the GPO settings can take effect.

The following sections follow through an example of the four steps. The example assumes a Windows 2008 server environment. Specific commands, options and actions may vary with the environment, and site group policy and security standards must of course be considered.

3.2.1 Create a Classifier Client Group

The first step is to create an Active Directory group containing all the Classifier client computers that are to forward events. This can be done by performing the following instructions.

1. Run **Active Directory Users and Computers,** in the left-hand pane, select **Computers,** and choose **New->Group** from the context menu.
2. Call the group something significant e.g. ***ClassifierClients***, set the Group scope to **Domain local** and the Group type to **Security**.
3. Press **OK** to create the group
4. Select the newly created group in the list of Computers in the right-hand pane of **Active Directory Users and Computers**, choose **Properties** from the context menu.
5. Select the **Members** tab and press **Add…**.
6. Press **Object Types…** and select ***Computers***.
7. Enter the name of all the Classifier client computers you want to add to the group and press **OK** twice.

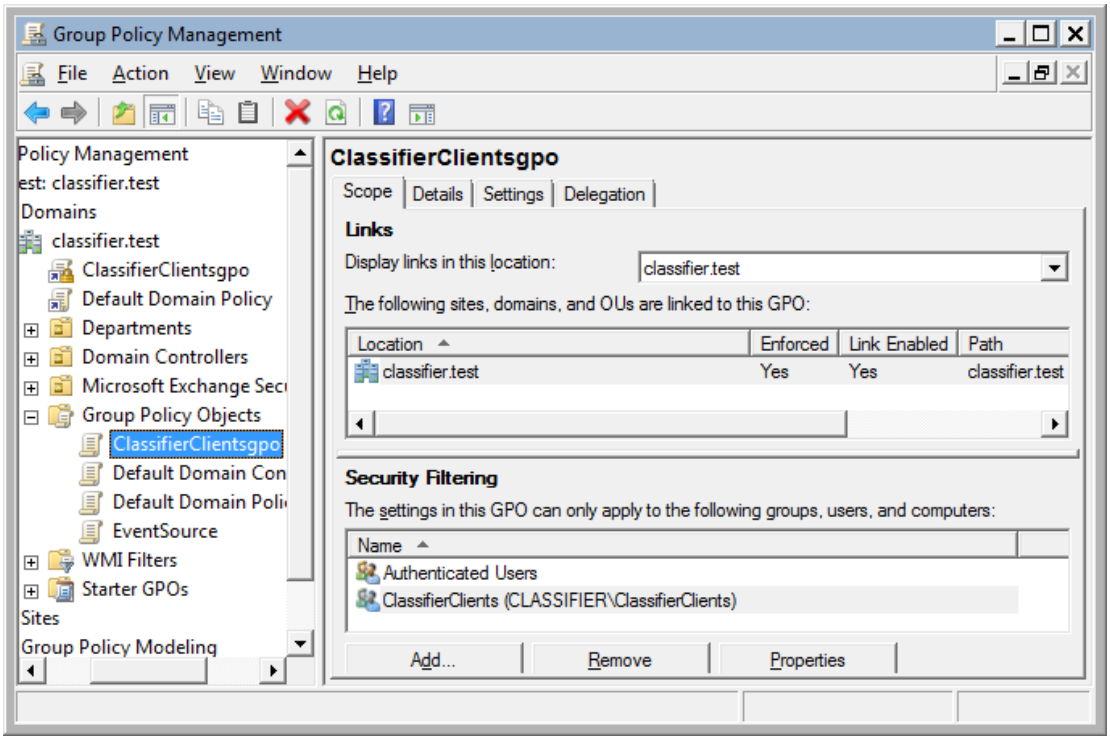
Note: Do not add the name of the Consolidated Event Log Server into the group.

3.2.2 Define a Group Policy Object for the Classifier Client Group

The next step is to create a Group Policy Object (GPO), apply it to the group created above (section Create a Classifier Client Group) and set policies on the GPO to collect and forward events. This can be done by performing the following instructions.

3.2.2.1 Create a GPO and apply it to the group

1. Using **Group Policy Management**, in the left-hand pane a tree of forests and domains is shown, expand the **Group Policy Management->Forest->Domains->*My Domain*** node.
2. Select the ***My Domain*** node, and choose **Create a GPO in this domain, and Link it here…** from the context menu.
3. Enter a name for the GPO, (e.g. ***ClassifierClientsgpo)*** and press **OK**. This will create a new GPO that is shown in the **Group Policy Management -> Forest ->Domains->*My Domain*->Group Policy Objects** node.
4. Select ***ClassifierClientsgpo*** and details of the ***ClassifierClientsgpo*** will be displayed in the right-hand pane.
5. Set **Enforced** to **Yes**, **Link Enabled** should already be set to **Yes**.
6. Press **Add** and add the ClassifierClients group created above (in section Create a Classifier Client Group). This applies the GPO to the group.



Group Policy Object

3.2.2.2 Set policies on the GPO

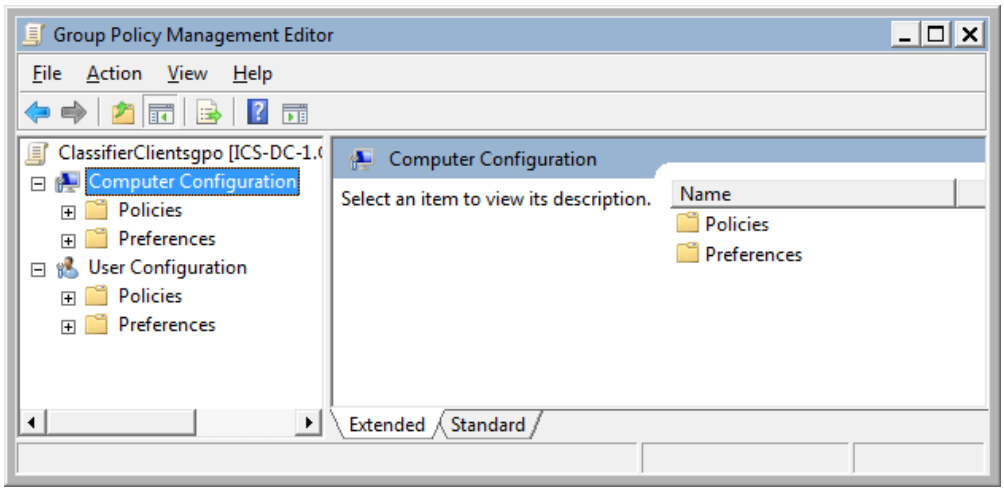
This section explains how the GPO created in section Create a GPO and apply it to the group should be configured to enable event forwarding. The following needs to be configured.

- The WinRM service should be started.
- Event Forwarding should be enabled
- The WinRM process should be given permission to read event logs.

These will be discussed in turn together with security concerns in this section

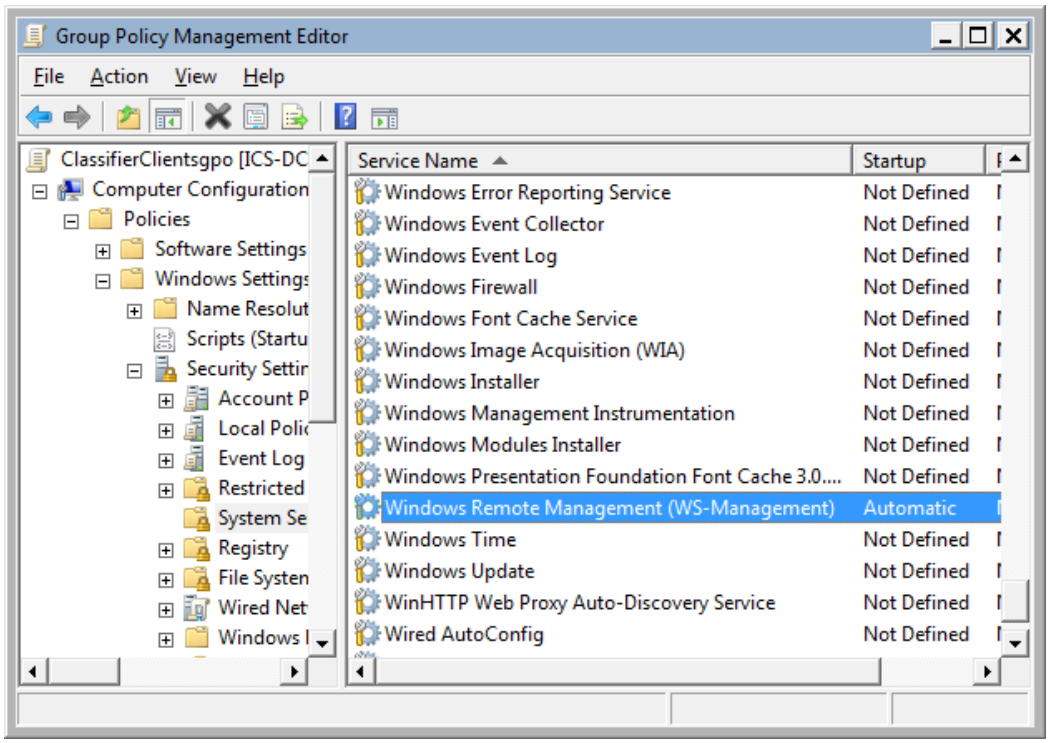
3.2.2.3 Enable the WinRM service

1. Using **Group Policy Management** select the ***ClassifierClientsgpo*** object defined in section Create a GPO and apply it to the group. Choose **Edit**.



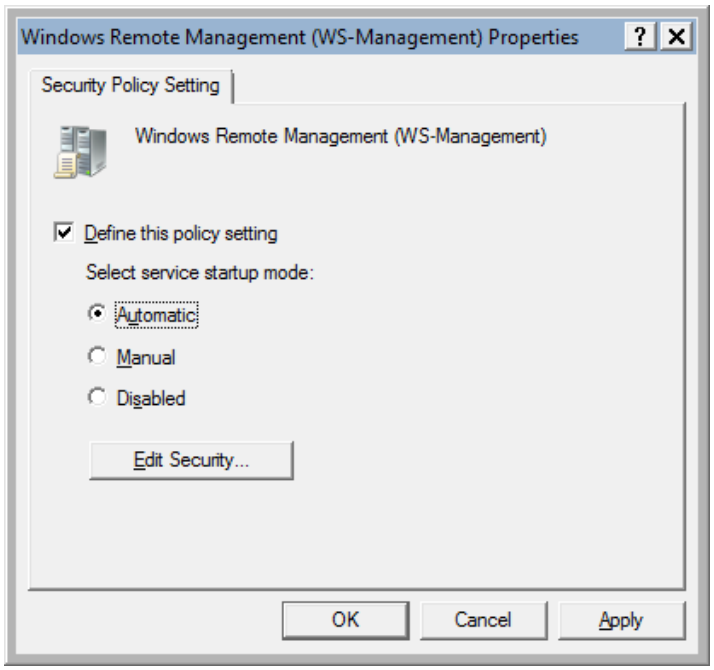
Edit ClassifierClientsgpo

2. On the tree on the left-hand side select **Computer Configuration->Policies->Windows Settings->Security Settings->System Services** and then select the item **Windows Remote Management (WS-Management)** from the list on the right-hand side.



Windows Remote Management policy setting

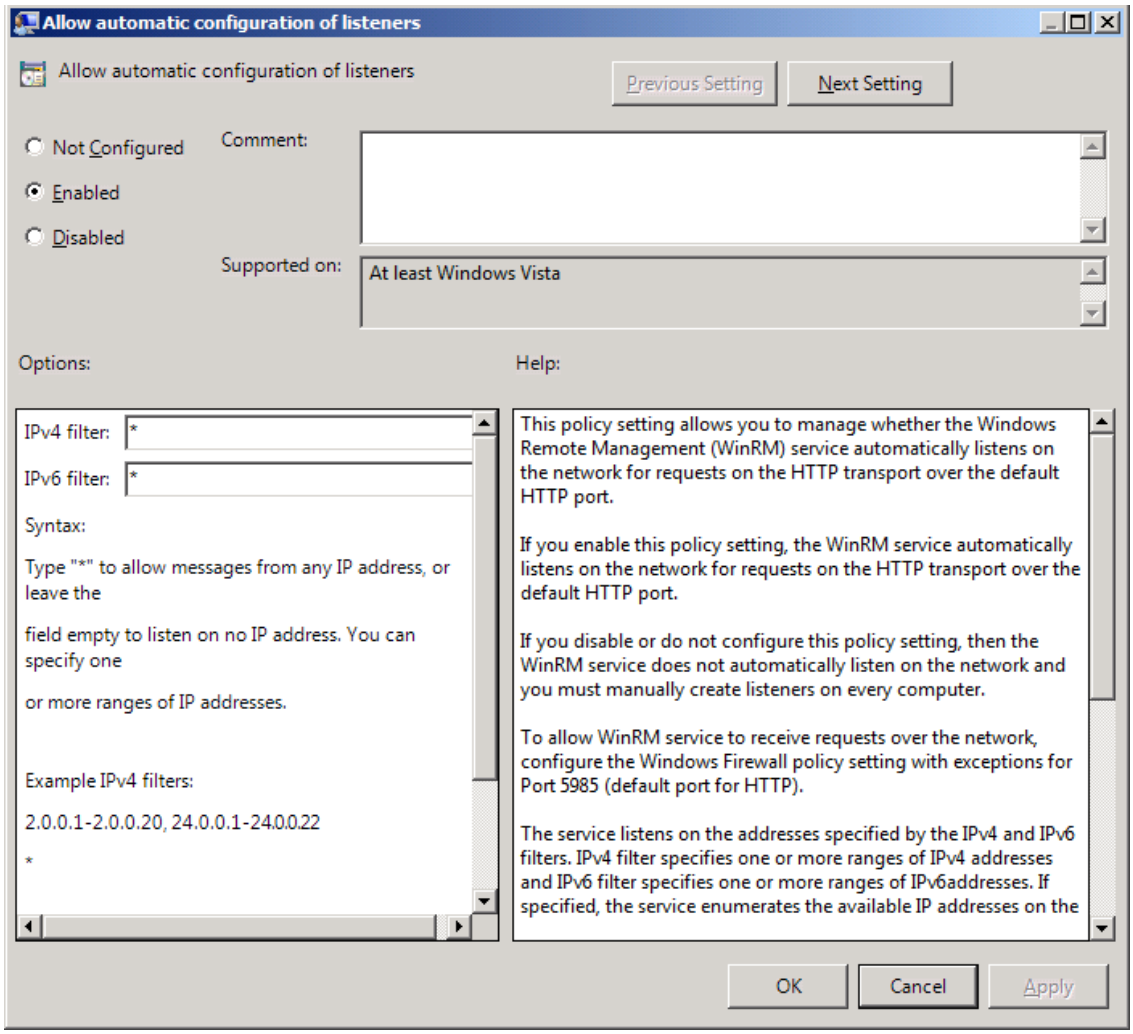
3. Choose **Properties** from the context menu. The **Windows Remote Management (WS-Management) Properties** dialog will be displayed.



Windows Remote Management (WS-Management Properties)

4. Check **Define this policy settings** and set **service startup mode** to **Automatic**. Press **OK**.
5. On the tree on the left-hand side of **Group Policy Management** select the node **Computer Configuration->Policies->Administrative Templates->Windows Components->Windows Remote Management (WinRM)->WinRM Service.**
6. On the right-hand pane select **Allow automatic configuration of listeners,** select **Edit** the policy setting. The **Allow automatic configuration of listeners** dialog is displayed.

   (The policy setting for 2012 is **Allow remote server management through WinRM**.)



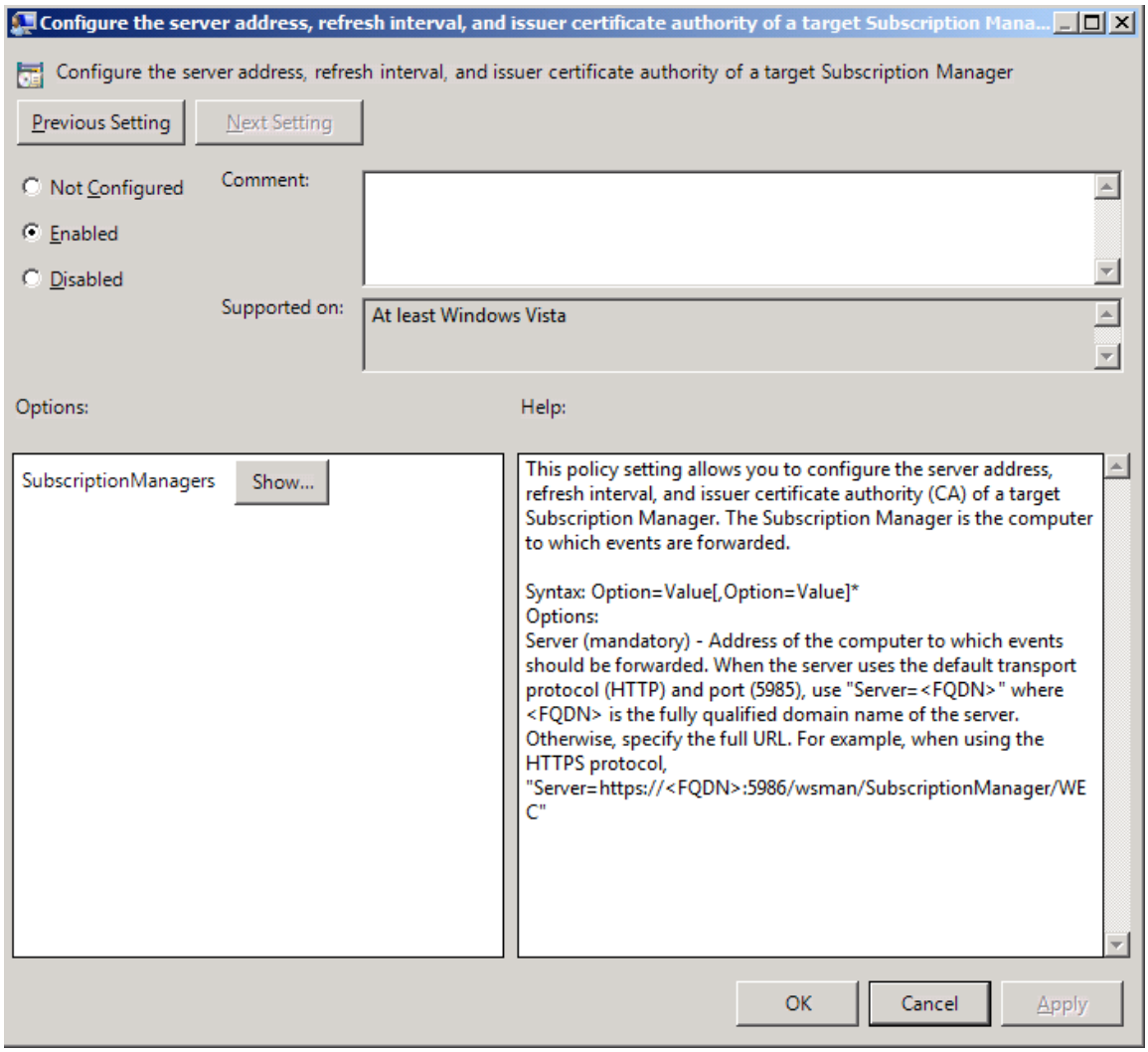
Allow automatic configuration of listeners

7. Select **Enabled** and set both the **IPV4 and IPV6 filter** value to *.
8. Press **OK**.

3.2.2.4 Enable Event Forwarding

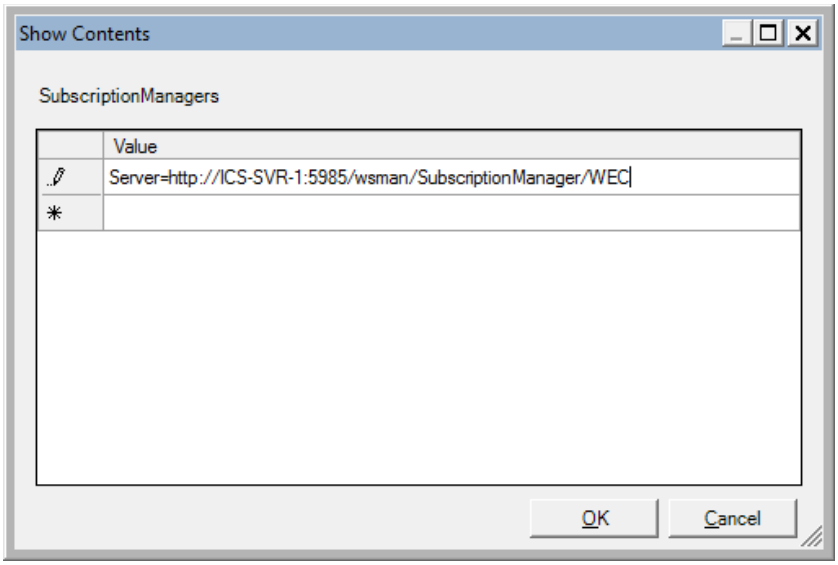
1. Using **Group Policy Management** select the policy object defined in section Create a GPO and apply it to the group
2. Select the node **Computer Configuration->Policies-> Administrative Templates->Windows Components->Event Forwarding.**
3. On the right-hand pane select **Configure the server address, refresh interval, and issuer certificate authority of a target**, and **Edit** the policy setting. The **Server Configuration** dialog is displayed.

   (The policy setting for 2012 is **Configure target subscription manager**.)



Server Configuration

4. Select **Enabled**
5. Press **Show…** and the **SubscriptionManagers** dialog is displayed.



Subscription Manager

6. A Server entry should be added in the first row. Place the mouse into the row and enter the following

   Server=http://MyServer:5985/wsman/SubscriptionManager/WEC

Note: You must enter all the text including "Server="

Where:

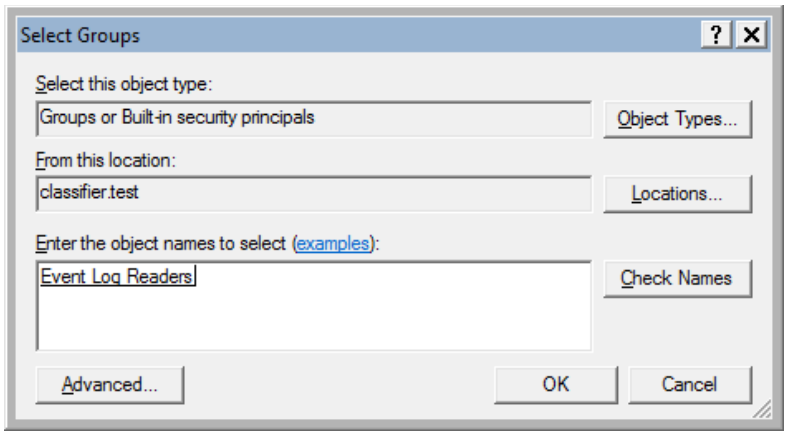
- ***MyServer*** is either a full-qualified domain name or a hostname for the server which is to collect the forwarded events.
- **5985** is the port that WinRM communicates over.

7. Press **OK** to close the **SubscriptionManagers** dialog.
8. Press **OK** to close the **Server Configuration** dialog.

3.2.2.5 Set WinRM permissions

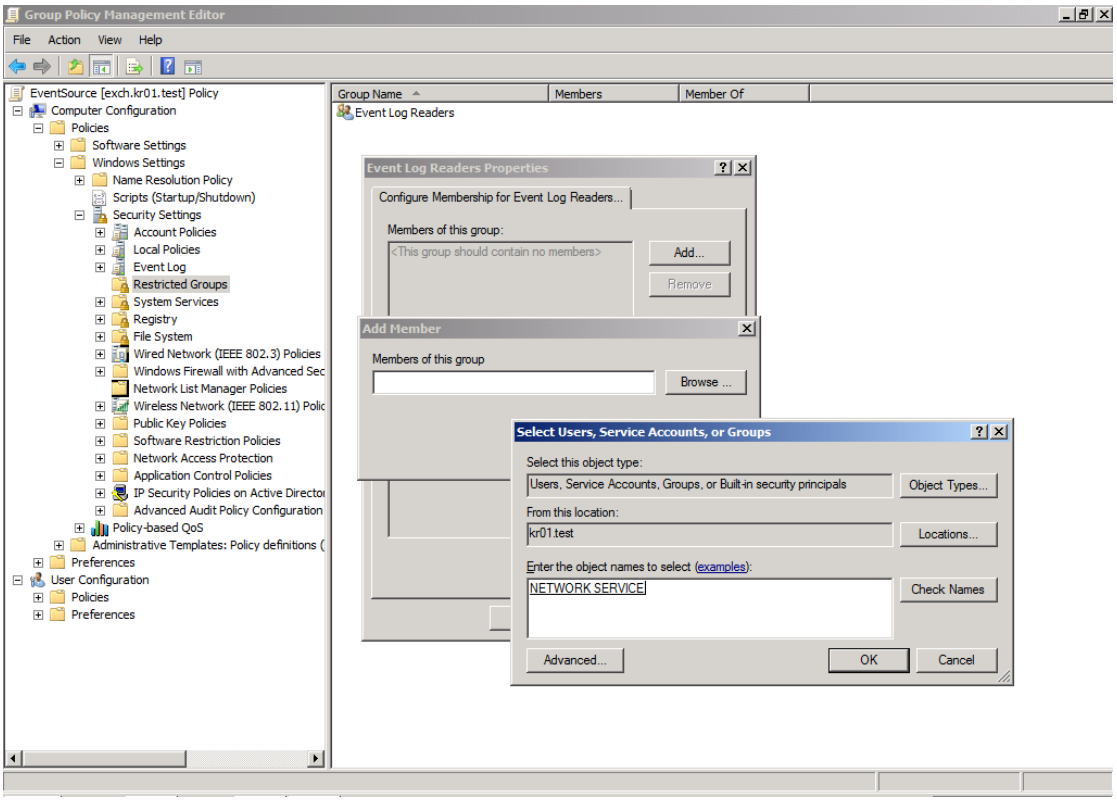
The WinRM service runs under the **Network Service** account. So that the WinRM service can read event logs the **Network Service** account has to be added to the **Event Log Readers** Group. Doing this by GPO is a two-stage process. Firstly, the **Event Log Readers** group has to be added to the Restricted Groups in the GPO and then the **Network Service** account has to be added to the **Event Readers** group.

1. Using **Group Policy Management** select the policy object defined in section Create a GPO and apply it to the group. Choose **Edit**.
2. Select **Computer Configuration->Policies-> Windows Settings->Security Settings->Restricted Groups, and choose Add Group…** from the context menu.



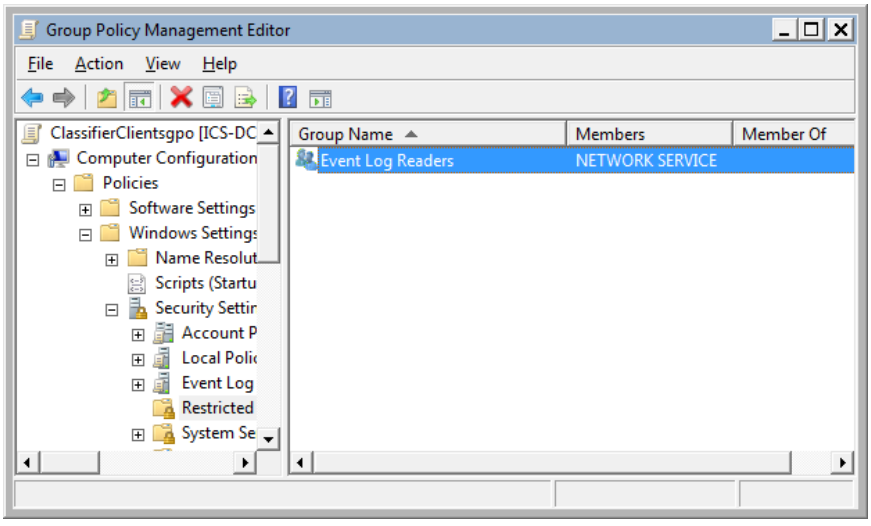
Event Log Readers

3. Press the **Add** button and then press the **Browse** button and add the **Event Log Readers** group by using the **Select Groups** dialog.
4. Press **OK** (three times) and the **Event Log Readers** group is now displayed in the right-hand side of the **Group Policy Management Editor**.
5. Select **Event Log Readers** choose **Properties** from the context menu. The **Event Log Readers Properties** dialog will be displayed.



Event Log Readers Properties

6. Press the **Add** button (at the top of the dialog) and then press the **Browse** button and add the **Network Service** group by using the **Select Users, Service Accounts, or Groups** dialog.
7. Press **OK** (three times) and the **Event Log Readers** group, showing **Network Service** as a member will be displayed in the right-hand pane of the **Group Policy Management Editor**.



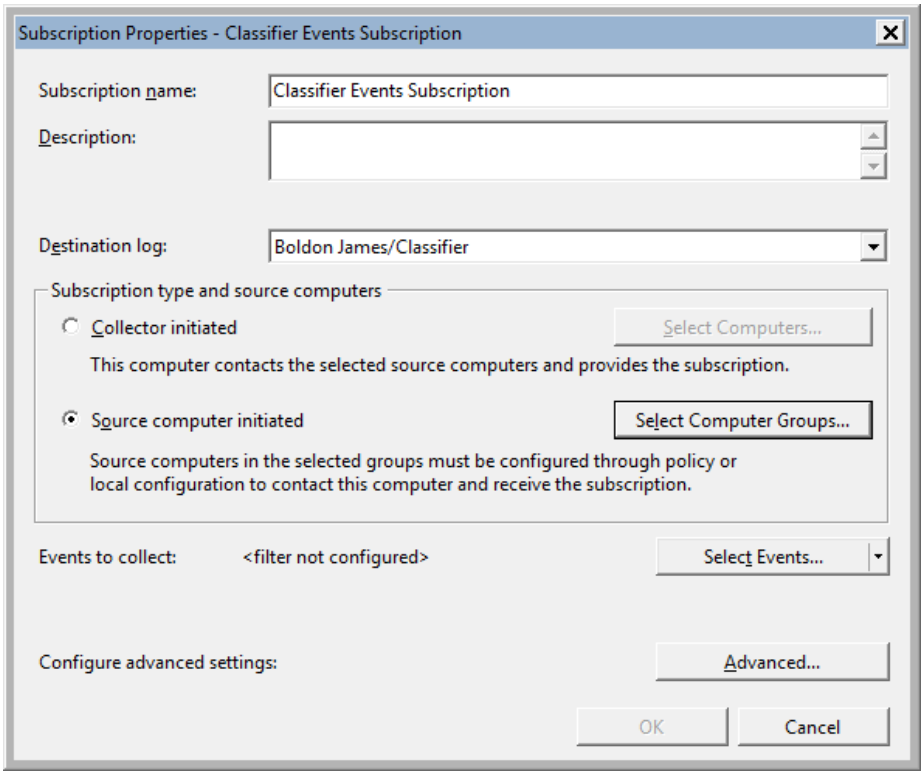
Event Log Readers added to Restricted Groups

3.2.3 Define a Classifier Events Subscription

A subscription should be defined to collect events from Classifier client computers on the Consolidated Event Log server (this server should also host the Classifier Reporting Event Log service). This section will explain how this can be done.

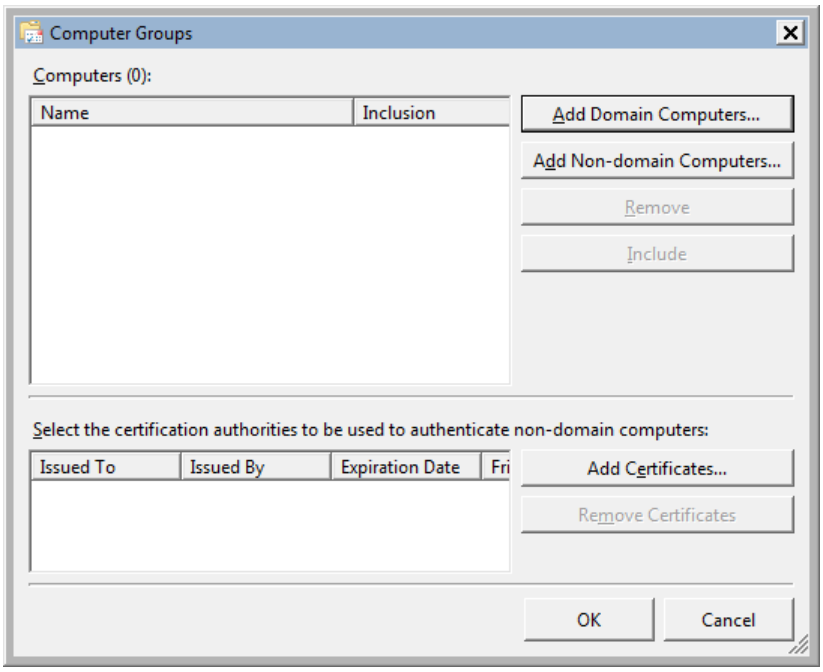
1. Start **Event Viewer** and select the Subscriptions node and choose “Create Subscription…” from the context menu. The **Subscription Properties** dialog will be displayed.

Note: If this is the first Subscription to be created you will be prompted that the Windows Event Collector Service must be running. Press Yes and Services will be displayed allowing you to start the service.



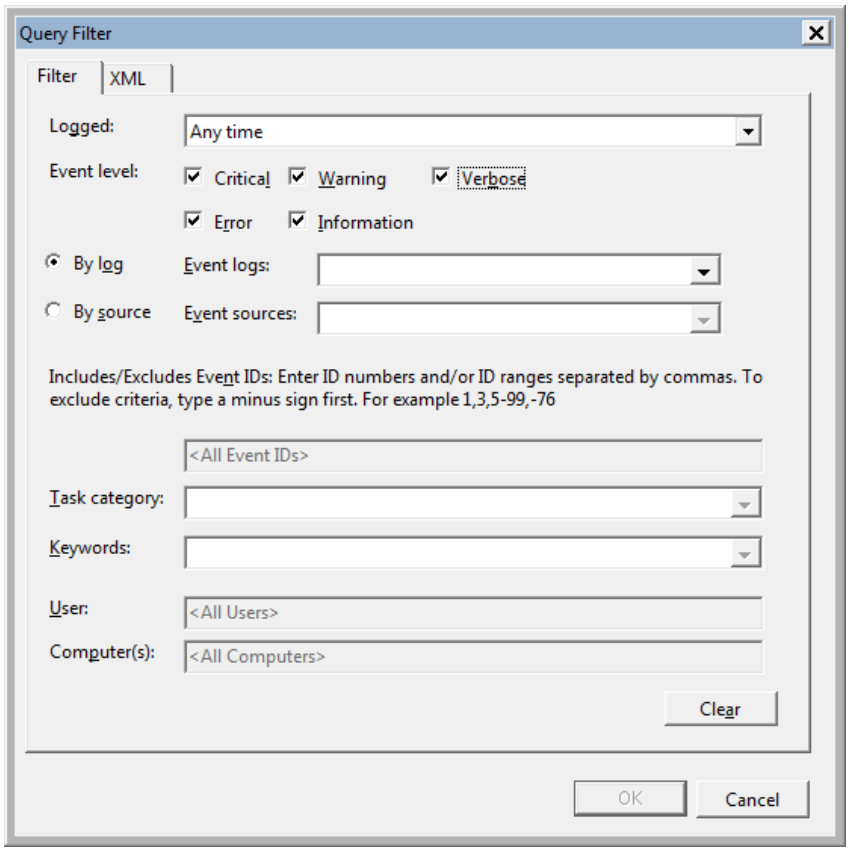
Create Events Subscription

2. Provide a name for the subscription, for example “**Classifier Events Subscription**”.
3. Select the **Boldon James/Classifier** event channel from the **Destination log**: drop-down list. The **Boldon James/Classifier** event channel is created if you install the Event Log Service. Alternatively, if you wish to collect events to a server without installing the service you can create the channel by running the Event Channel Wizard.
4. Select **Source computer initiated**.
5. Press **Select Computer Groups…** the **Computer Groups** dialog is displayed



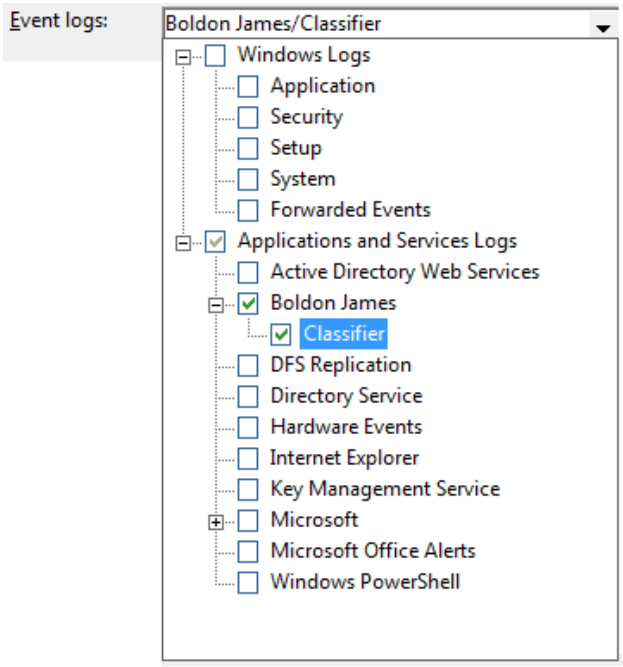
Computer Groups

6. Press **Add Domain Computers…** and select the computer group created in section Create a Classifier Client Group (e.g. ClassifierClients).
7. Press **OK** (twice) and return to the **Subscription Properties** dialog.
8. Press **Select Events…** and the **Query Filter** dialog is displayed



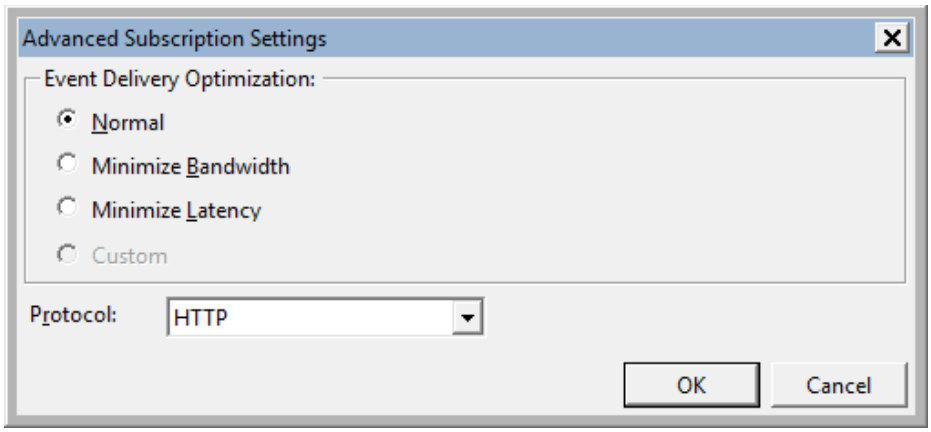
Event Subscription Filter

9. Select all the **Event level** check boxes.
10. Select **By log** and then select **Boldon James/Classifier** event channel in the **Event Logs** dropdown as shown below.



Choose Event logs

11. Press **OK** to return to the **Subscription Properties** dialog.
12. Press **Advanced** and the **Advanced Subscription Settings** dialog is displayed



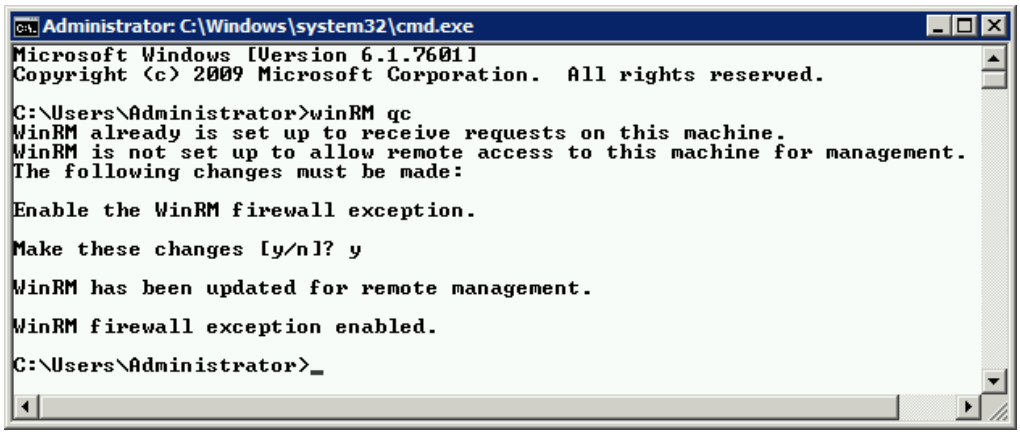
Advanced Subscription Settings

(Normal – 15 minutes, Minimize Bandwidth – 6 hours and Minimize Latency - 30 seconds)

13. Set **Protocol** to **HTTP**.
14. Press **OK** to return to the **Subscription Properties** dialog.
15. Press **OK** to complete the subscription.
16. Ensure that WinRM is operating and that the firewall allows events to be forwarded:

    From a Command prompt, run the following windows command:

    `winRM qc`



Run winRM qc

17. The events collected by this subscription must be collected in **Event** format not **RenderedText** format which is not usable by the Classifier Reporting database. To configure collecting in **Event** format run a Windows Command console and type:

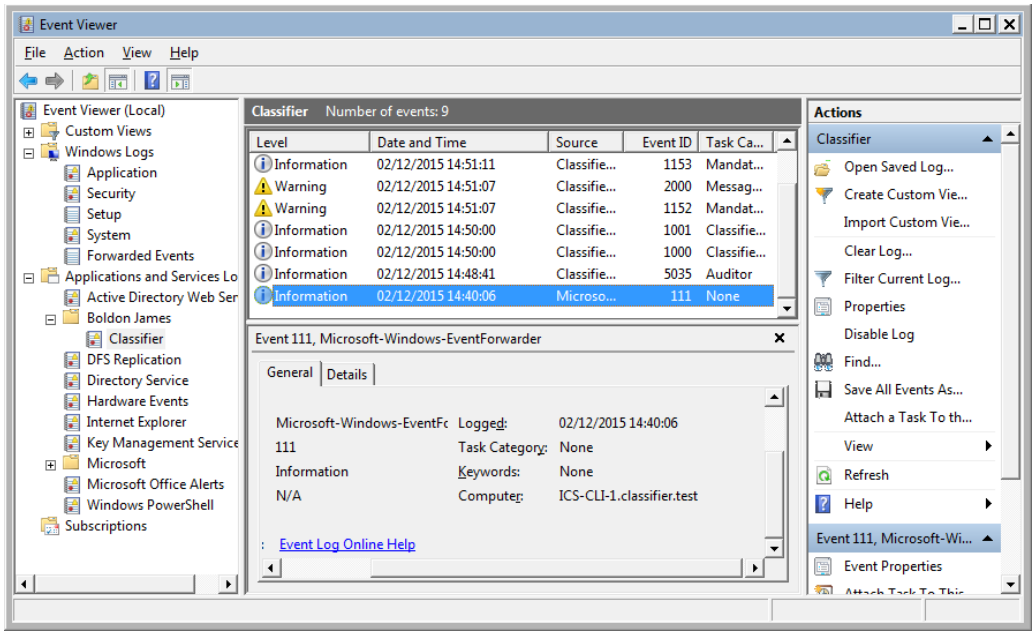
```
wecutil ss "Classifier Events Subscription" /CF:Events
```

Note “Classifier Events Subscription” is the name of the subscription created in step 2 above.

3.2.4 Re-start Client Computers

The final step is to restart all the Classifier client computers so that the changes to GPO can now take effect and configure the computers to start forwarding events.

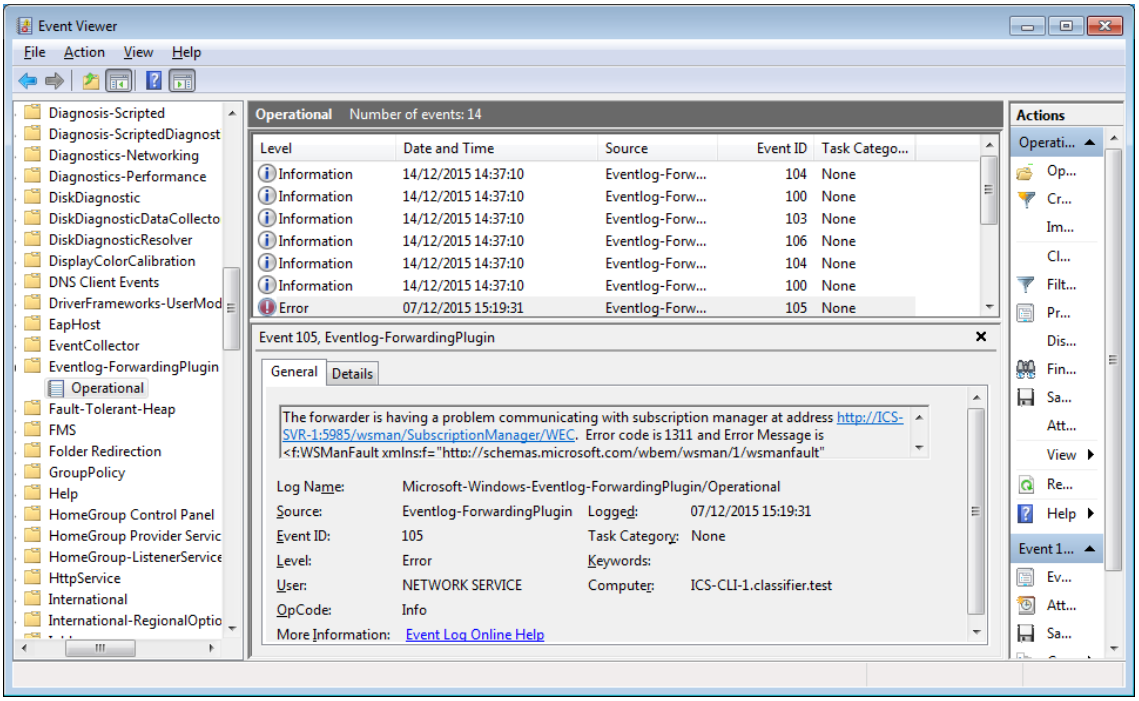
When a client computer initiates event forwarding, an entry (Event ID = 111) should appear in the Collector Event Viewer. Forwarded events will appear in due course (depending upon Latency set in **Advanced Subscriptions Settings** above, and of course Classifier events being generated on that computer).



Forwarded events received

Success and Errors (e.g. incorrect configuration) for submitting computers can be checked via:

Event Viewer > Applications and Services > Microsoft > Windows > Eventlog-ForwardingPlugin > Operational.

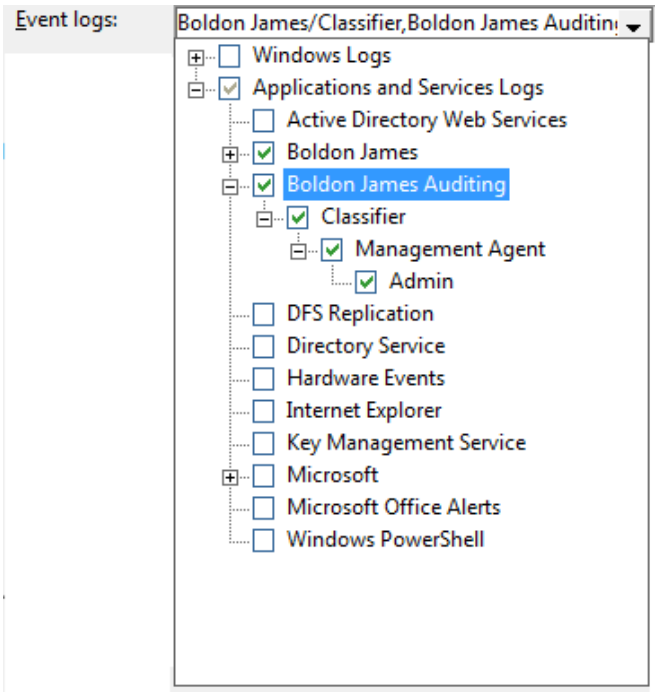


Source computer event forwarding logs

3.3 Forwarding Management Agent Events

If you deploy the Classifier Management Agent (MA) in your organisation, you may want to store the events it generates in the Classifier Reporting Database. MA events can be forwarded to the Consolidated Event Log server via the same subscriptions that forward Classifier events, or using separate subscriptions.

To collect MA events, select the **Boldon James Auditing/Classifier/Management Agent/Admin** event channel in the **Event Logs:** dropdown (equivalent to item 8 in section Consolidate Event Log Servers) when defining the Event query filter as shown below



Choose Management Agent Event logs

The **Boldon James Auditing/Classifier/Management Agent/Admin** event channel is created if you install the Event Log Service. Alternatively, if you wish to collect MA events to a server without installing the service you can create the event channel on the collection server by running the Event Channel Wizard, see section Event Channel Wizard.

Note: The Boldon James Auditing/Classifier/Management Agent/Admin event channel is created by the MA on the Windows clients and is the location that the MA writes its events to. The MA events are forwarded to the Boldon James/Classifier event channel on the event collection server. However, the Boldon James Auditing/Classifier/Management Agent/Admin event channel has to be defined on the Event Collection Server so that a subscription can be defined to collect the events from the windows clients.

Note: Version 1.0 of the Classifier Reporting Services created an incorrect name for the Boldon James Auditing/Classifier/Management Agent/Admin event channel. If you have created this event channel you should remove it before you uninstall Version 1.0, by following these steps.

Run a command prompt with Administrator privileges and go to the C:\Program Files (x86) \Boldon James\Classifier Reporting Services directory.

Run the command: `wevtutil um bjManAgentEvents.xml`

3.4 Filtering Classifier Events

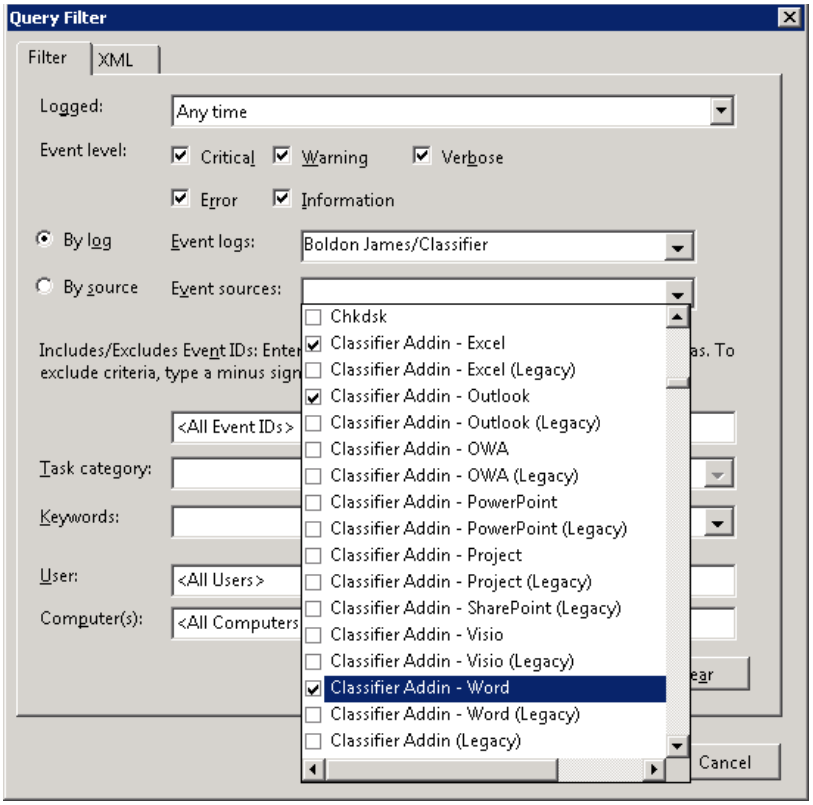
If you configure event forwarding according to the procedures described in this guide, all the events generated by all Classifier applications will be collected. It is possible to filter the events forwarded so that only events that you are interested in are transferred across the network and stored in the Classifier Events Database. For example, you may only want reports on email users and not

document users or you may only want to produce reports showing Classifier check rules that produced warnings or preventions.

There are two ways of filtering Events: using the Event Subscription Filter dialog or by defining a filter using XML. Both these methods will be briefly discussed in this section. Filtering classifier events can be configured for both Collector and Source initiated event forwarding.

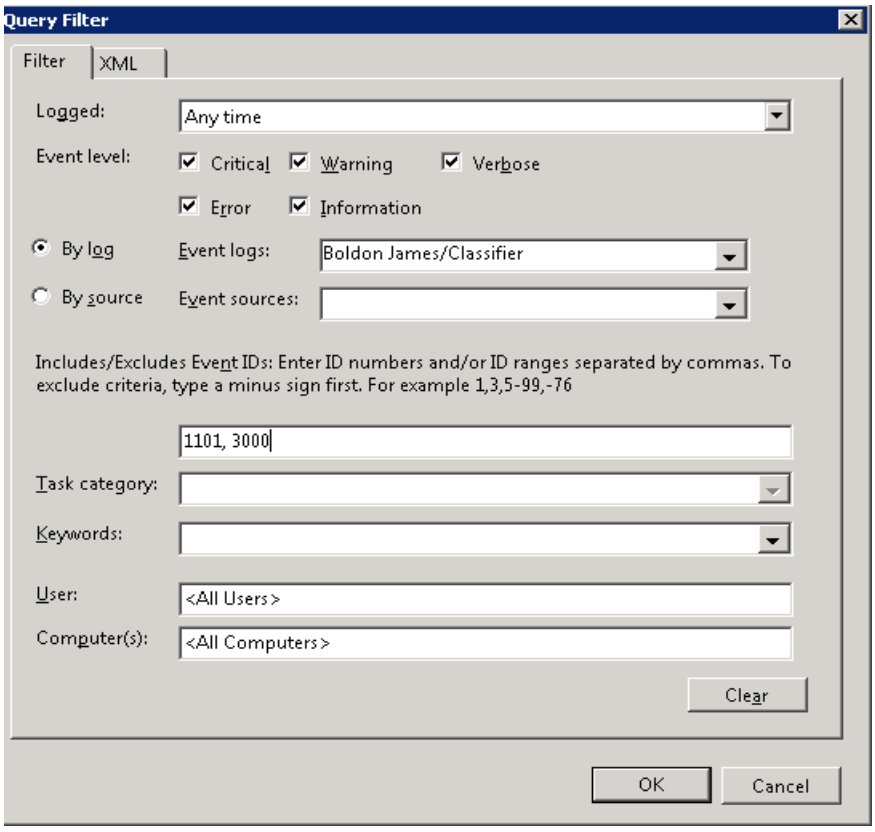
3.4.1 Event Subscription Filter dialog

The Classifier applications from which you wish to collect events can be configured by selecting items from the Event Source drop down on the Event Subscription Filter as shown below.



Query Filter dialog and Event Source drop down list

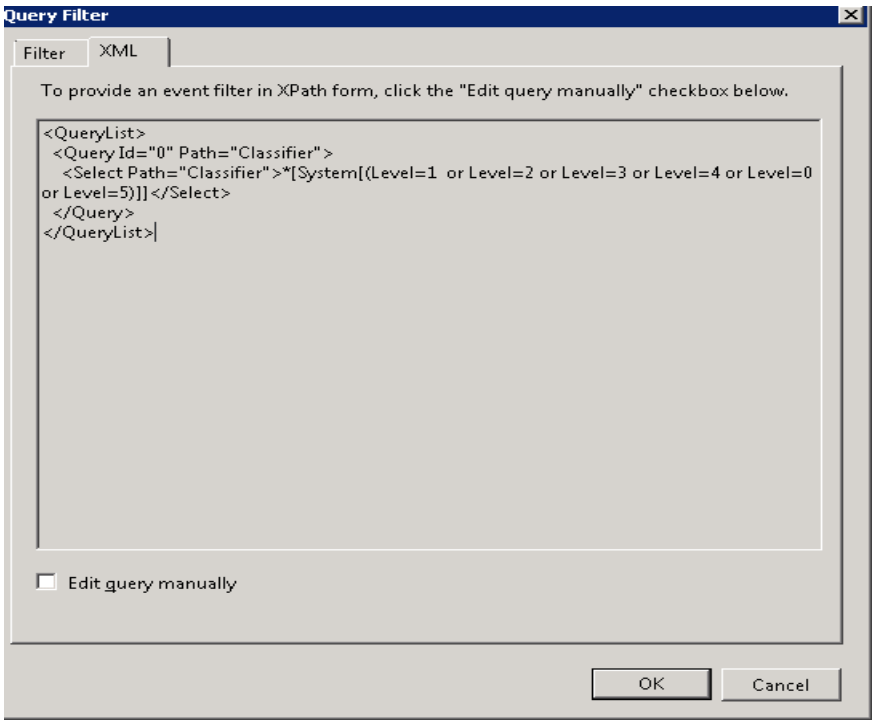
The Event Ids can also be selected. For example, if you only want to display the ***Email Sent by Classification*** and ***Documents Saved by Classification*** reports then you would only need to forward Events with Ids 1101 and 3000. This can be done by entering the Event Id as shown below. More information about Classifier event Ids is provided by the Classifier Administration Guide.



Query Filter dialog and Event Ids definitions

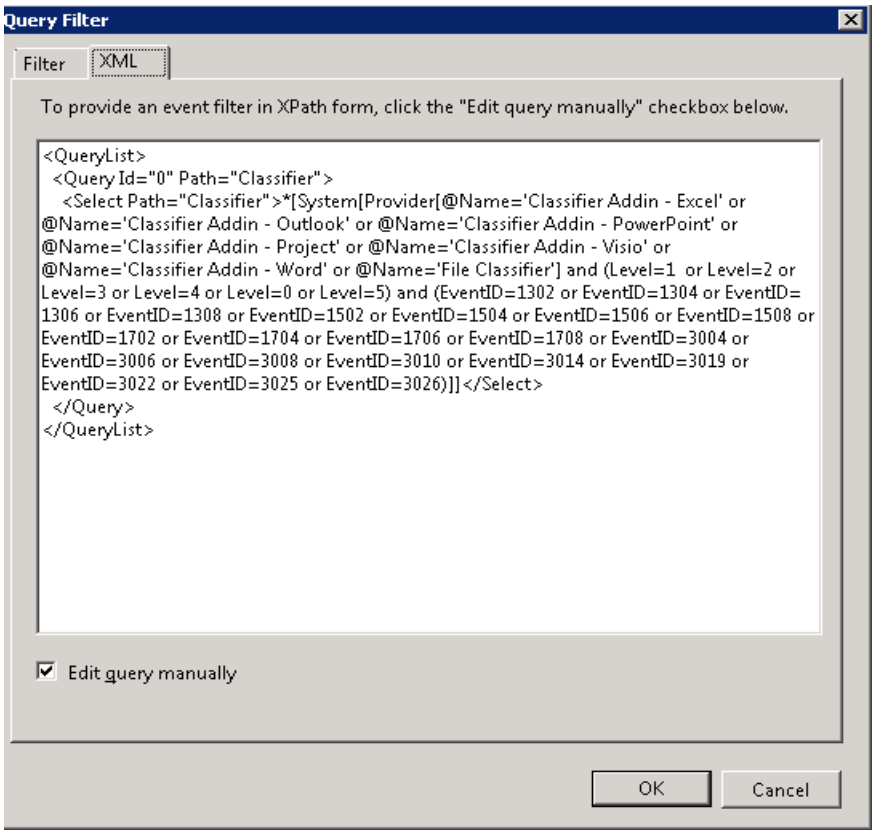
3.4.2 Defining an Event Subscription filter using XML

Event subscription filters are defined using XML. When a filter is defined on the Query Filter dialog, the XML definition of the filter can be viewed by selecting the XML tab as shown below.



Query Filter dialog and XML filter definition

It is possible to define an Event Subscription filter by directly adding a XML definition. To do this click the **Edit Query manually** check box as shown below. Note that you will be warned that if you do enter a XML definition that it is not possible to use the Event Subscription dialog for this subscription.



Query Filter dialog with a XML defined event subscription filter

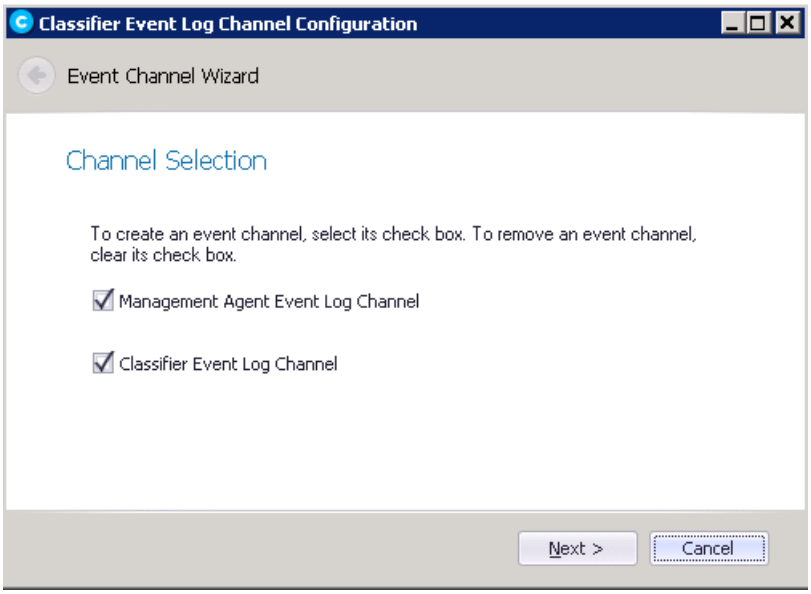
Several pre-defined XML filters that can be copied into the XML definition field as shown above, are provided with this release. These include the following.

ApplicationEvents.xml:	Collect Classifier events from Excel, Outlook, PowerPoint, Project, Visio and Word.
ApplicationAndErrorEvents.xml	Collect only error and warning Classifier events from Excel, Outlook, PowerPoint, Project, Visio and Word.
DocumentEvents.xml	Collect Classifier events from Excel, PowerPoint and Word.
DocumentAndErrorEvents.xml	Collect only error and warning Classifier events from Excel, PowerPoint and Word.
EmailEvents.xml	Collect Classifier events from Outlook, OWA and Notes.
EmailAndErrorEvents.xml	Collect only error and warning Classifier events from Outlook, OWA and Notes.
ManagementAgentEvents.xml	Collect only Management Agent Events.

3.5 Event Channel Wizard

The event channels needed to collect Classifier and MA events are created if the Classifier Event Log Service is installed. If you wish to collect events on a server where you have not installed the Service, the Event Channel Wizard can be used to create the two event channels instead. The Event Channel Wizard can also be used to delete the event channels as well.

To use the Event Channel Wizard, run the program ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services\ChannelWizard***



Channel Wizard

Select which channel you wish to create and click **Next**.

Note: The Classifier event channel will be automatically created on your system if you install the Event Log Channel Wizard even if you do not also install the Event Log Services.

Note: The event channels are not automatically deleted if you uninstall the Event Log Services but you can delete the channels using the Event Channel Wizard.

3.6 Event Forwarding Trouble Shooting

For the benefit of this troubleshooting guide, the following terms are defined:

- **Collecting machine** – this is the machine where the Event Log subscription is setup (typically where the Classifier Reporting Event Log service runs)
- **Forwarding machine(s)** – these are the computers where events are forwarded to the Collecting machine

There will typically be one collecting machine and very many forwarding machines.

Issue	**Note**
Basic checks	Note that it can take over 15 minutes for events to be forwarded in standard operation. You may wish to set “Minimize Latency” from the

Issue	Note
	Advanced dialog of the Subscription in evaluation stages to ensure events are forwarded more frequently (every 30 seconds).
Basic checks	Note that previously generated events on the forwarding machines **are not** forwarded when a subscription is set up in standard mode. You **must** generate new Classifier events on the forwarding machines ***after*** the subscription has been set up.
Basic checks	Ensure that there is network connectivity between the collecting machine and the forwarding machine using standard tools such as **ping** and **nslookup** for DNS.
Basic checks	On the collecting machine, ensure that the subscription is Enabled by checking the status in the subscriptions section of the Event Log.
Basic checks	On the collecting machine, ensure that the Runtime Status of the subscription indicates that the forwarding computer is “Active”. If this is not the case, follow the steps below.
The collecting machine subscription “Runtime status” indicates “The client cannot connect to the destination…”	This suggests that the Windows Remote Management service is not running, or is not accessible, on the forwarding machine. See below for resolution.
The collecting machine subscription “Runtime status” indicates “Access is denied”	This indicates that the account used to run the subscription does not have permission to access the forwarding machine event logs. Check the account used to run the subscription (from the Advanced button on the subscription properties). You will need to give this account permission to the forwarding computer event log as described above in Section 3.2.2.5.
Basic checks	On the forwarding machine, check the **Applications and Services Logs/Microsoft/Windows/Eventlog-ForwardingPlugin/Operational** event log to see if the subscription has been successfully set up. If you have no event in this event log it is likely that winrm is not running on the forwarding machine, or that you have firewall issues. An event with id 100 indicates that the subscription has been set up. The event detail will confirm the name of the subscription that has been set up. An event of id 102 indicates an error. Typical problems include: – Incorrect channel name in subscription – Authentication issues

Issue	Note
Checking collecting machine configuration	If the above step indicates a problem, verify that the event query is valid by performing these steps on the collecting computer: 1. View the subscription properties, and click Select Events… 2. On the XML tab, copy the contents of the query 3. Open a second instance of Event Viewer. 4. Right-click the Event Viewer, and then select Connect to Another Computer... Enter the hostname of the forwarding computer in the Another computer text box. 5. Right-click Custom Views, and select Create Custom View… 6. Select the XML tab. Click the 'Edit query manually' check box, and click Yes when prompted. 7. Click the query box and paste the previously copied query. Click OK. 8. The new custom view appears and shows the matching events. If there are no events shown the query is incorrect. If events are shown, then the forwarding mechanism is failing If there are no events shown in the above step, note that the Path element in the query should be "**Classifier**" for Classifier client events, and "**Boldon James Auditing-Classifier-Management Agent/Admin**". Be especially careful with the placement of the dashes, spaces and the slash. If there are events shown but they are not being forwarded, check that the Windows Remote Management service is running on the forwarding machine. On the forwarding machine, type in a console window: **winrm enumerate winrm/config/Listener** If this returns with no output, it is likely that you have not set up the service. Execute, on the forwarding machine: **winrm quickconfig**
Checking forwarding machine configuration	From the collecting machine, check that you can connect to the WinRM service on the forwarding machine. In a console window type: **winrm id -remote:<forwardingmachine>.<yourdomain>.<com>** This should return with an IdentifyResponse indicating ProtocolVersion etc. If the return indicates "…client cannot connect to the destination…" then it is possible that there are firewall issues.
winrm to forwarding machine cannot connect	On the forwarding computer, ensure that HTTP-In (typically port 80) or HTTPS (typically port 443) exceptions are available in your chosen firewall configuration. Running **winrm quickconfig** will set up the appropriate firewall exceptions for MS firewalls.
winrm to forwarding machine cannot connect	On the collecting machine, ensure that HTTP-In for Windows Remote Management (typically port 5985) exception is available in your chosen firewall configuration.
Events are	If you are getting events forwarded but they are not being processed by

Issue	Note
being forwarded but not processed	the Classifier Reporting Event Log service, ensure that the subscription is requesting events in Events format. On the collecting machine, in a console window, execute: **wecutil gs "Your subscription name"** [NB: run **wecutil es** to list your subscriptions] Check that the **ContentFormat** is listed as "**Events**" If this is not the case, execute **wecutil ss "Your subscription name" /CF:Events** Note that this is only effective for new events forwarded to the collector.
I'm expecting to see more events in my reports	Finally, if you have events in the Classifier Reporting database but you expected more events, have you set up a filter on the subscription for particular events? Check the subscription Select Events… dialog and review the filter.

4 THE CLASSIFIER REPORTING DATABASE

This section explains how the Classifier Reporting Database can be created and explores some features of the database. If you are upgrading an existing database refer to section Upgrading the Classifier Reporting Database below.

4.1 Creating the Classifier Reporting Database

The SQL Server Database has to be created to store and process event log data. This is done by installing the **Database Management** component of Classifier Reporting Services and then either running the PrepareDatabase program or by loading a set of scripts into **SQL Server Management Studio**. Both methods will be discussed in this section.

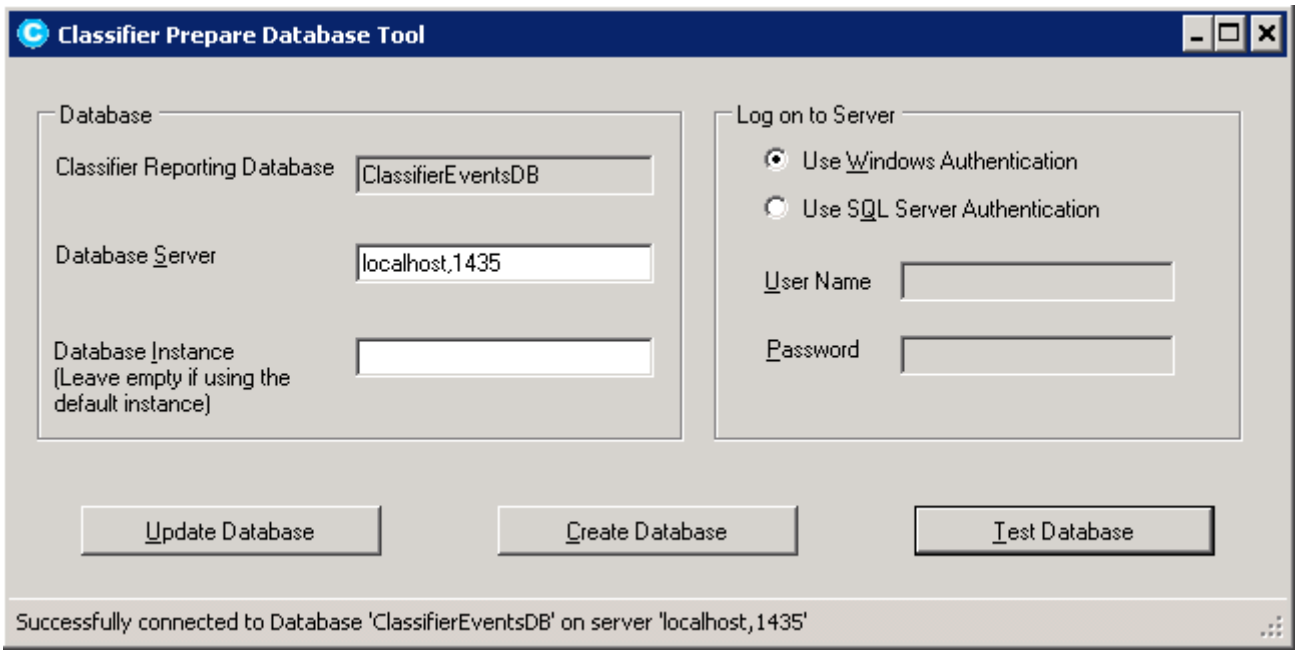
4.1.1 Creating the Classifier Reporting Database by running PrepareDatabase

The Classifier Reporting Database can be created by running the PrepareDatabase program. You can use either Windows Authentication or SQL Server Authentication to create the database.

To create the Classifier Reporting Database complete the following steps.

1. Ensure you have an installed and correctly working version of SQL Server 2008 or later with SQL Server Agent service running.
2. If you want to use Windows Authentication log onto Windows as a User who has sysadmin Server Role privileges in the SQL Server database.
3. If you want to use SQL Server Authentication create a Login for the database in **SQL Server Management Studio** and grant the Login the sysadmin Server Role
4. Run PrepareDatabase by running the file

   C:\Program Files (x86)\Boldon James\Classifier Reporting Services\PrepareDatabase
5. Enter the name of the server running the Classifier Reporting database. This should be ***localhost*** as shown in the picture above, if you are running the program from the server that hosts the SQL Server.



6. If your SQL Server is not listening on the default TCP port for SQL Server you will need to enter the port, that the SQL Server is listening on, to the server name; enter ***Server Name, Port.*** For example to create a Classifier Reporting database on a server called *myhost* on port 1435, enter ***myhost,1435*** in the Database Server field.
7. If you want to create the Classifier Reporting database in a SQL Server instance other than the default (unnamed) instance, enter the name of that instance into the **Database Instance** field. You do not need to enter an instance name if you want to create the Classifier Reporting database in the default instance.
8. Select either ***Use Windows Authentication*** or ***Use SQL Server Authentication***. If you use SQL Server Authentication, then you must also enter a ***User Name*** and ***Password***.
9. Press ***Create Database***. This runs a set of SQL scripts that creates the Classifier Reporting Database.
10. When the process is finished, you should test whether the Classifier Reporting Database has been successfully created by pressing ***Test***.
11. The Database Management program creates a text file showing the progress of the creation process. If there is a problem creating the database, you can check the file for details. The file is **C:\Users\<UserName>\AppData\Local\Temp\PrepareDatabase.log**

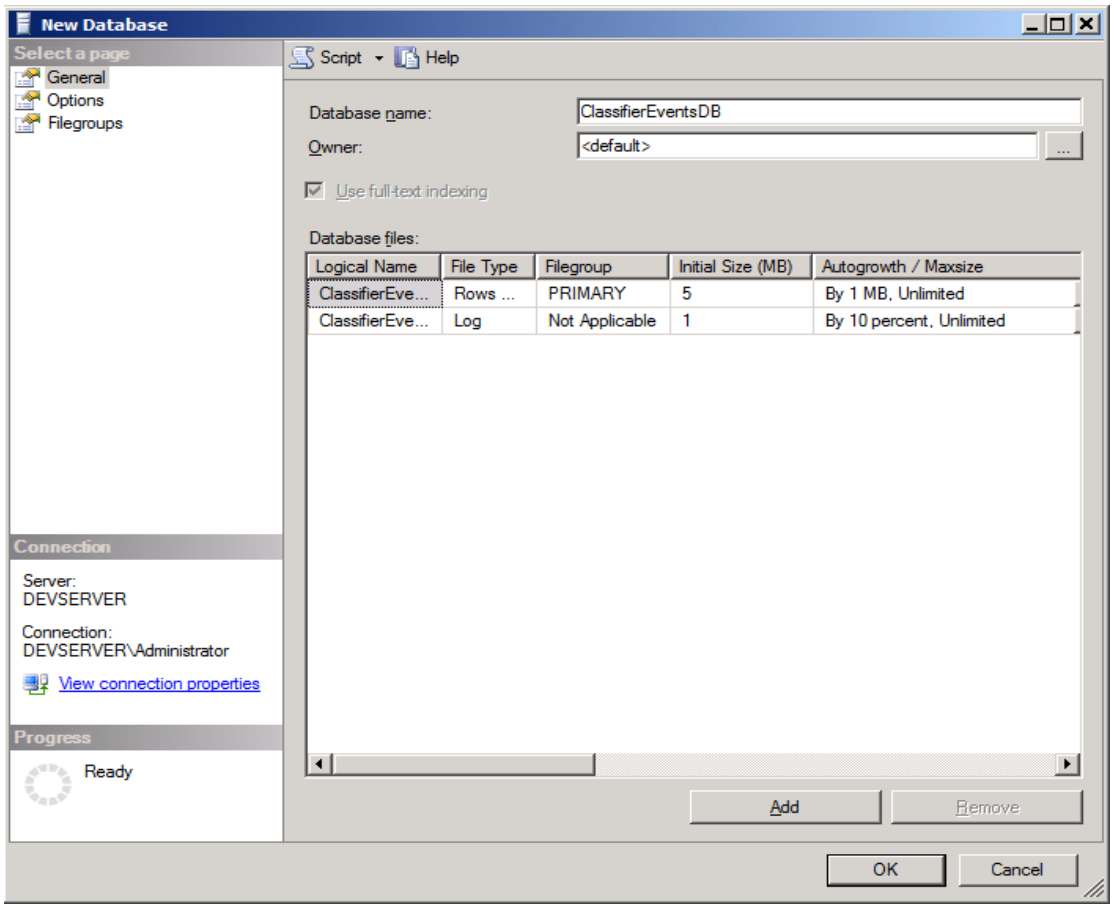
4.1.2 Communication between PrepareDatabase and the SQL Server

PrepareDatabase communicates with the SQL server using TCP/IP on the standard SQL port or on another port specified by the user. The SQL Connection string to communicate with the Server is constructed by PrepareDatabase. If you wish to communicate directly with the SQL server or wish to inspect the SQL scripts run by PrepareDatabase you can create the Classifier Reporting database by running the SQL in the SQL Server Management Studio itself. This is explained in the next section.

4.1.3 Creating the Classifier Reporting Database by running SQL Script files

To create the Classifier Reporting Database by running SQL scripts complete the following steps.

1. Ensure you have an installed and correctly working version of SQL Server 2008 or later with SQL Server Agent service running.
2. Ensure that you are logged on to Windows as a User who has sysadmin Server Role privileges in the SQL Server database.
3. Start **SQL Server Management Studio**, on the tree on the left-hand side, select the **Databases** node, choose **New Database…** from the context menu and call the new database ***ClassifierEventsDB.*** Press **OK** to create the database.



Creating ClassifierEventsDB Database

4. When the database has been created select **File->Open** from the **File** menu and navigate to the directory ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services\SQL*** that contains the SQL scripts.

5. All the script files have names of the form

   <nn><description>.sql

   Where <nn> is a number indicating the order that the scripts should be run. For example, the script **01 Create Database.sql** should be run first followed by **02…sql** and so on.

   After opening the scripts, they should be run by pressing the **Execute** button on the **SQL Server Management Studio** toolbar.

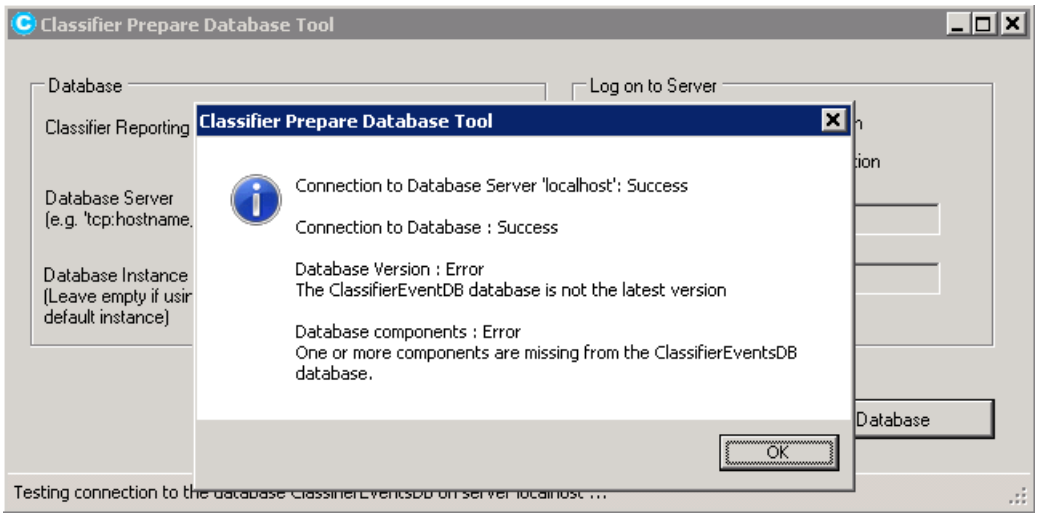
   If the scripts are run in the prescribed order they should run successfully. There may be some warnings if the SQL Server Agent is not running (see the section Automatic Event Processing and Deletion) but the warnings can be ignored.

5 UPGRADING THE CLASSIFIER REPORTING DATABASE

5.1 Updating from a Version 1.0 database to a Version 1.2 database

If you have an existing version 1.0.0 or version 1.1.0 database you **must** upgrade the database to use the new features in version 1.2.0 such as labels in events being parsed into selector values. You should also update installations of your Reporting Console to version 1.2.0.

1. Uninstall all instances of the Classifier Reporting Console from previous versions of the Reporting System
2. Stop the Event Log and Active Directory Service(s). Stop all instances of the Classifier Event Log Service so that events are not being processed as the migration happens.
3. Uninstall the services and all additional utilities supplied with the older versions of the Reporting System
4. Run Staging to Working stored procedures (usp_DocumentEventsWorkingInsert and usp_EmailEventsWorkingInsert) in Microsoft SQL Server Management Studio. These procedures move database entries from the Staging to the Working tables. The migration wizard only operates on the Working table data so it is important to move all your existing events to the Working tables' area. Note that you may continue to have events in the Staging tables after running the stored procedures. This is not unexpected.
5. Install the Event Log Service and Active Directory Services (if using) and all required additional utilities. Do **NOT** start the services.
6. Run the new Prepare Database program. Enter the name of the server running the SQL Server database and the appropriate authentication details.
7. Press the ***Test*** button. The following message will be displayed if the Classifier Reporting database needs updating.



Database Version Warning

8. If the Test button identifies that the database version is not the latest version, then press the ***Prepare Database*** button
9. Re-run the new Staging to Working stored procedures that are installed as part of the PrepareDatabase process. This will move any Classifier client events that were not recognised by the older Classifier Reporting database to the Working area.
10. Run the migration wizard

    See the section Migration Wizard**.** The migration wizard will parse the classification values in your existing Working table entries.
11. Start the new Event Log and Active Directory (if using) Services
12. Install and configure the latest version of the Classifier Reporting Console onto the relevant endpoints

5.1.1 Migration Wizard

If you have an already populated database from versions 1.0 or 1.1 of the Classifier Reporting Services, you will need to update the database to version 1.2 using the database migration wizard. **You do not need to run the migration wizard to update the database from version 1.2 to a later version**.

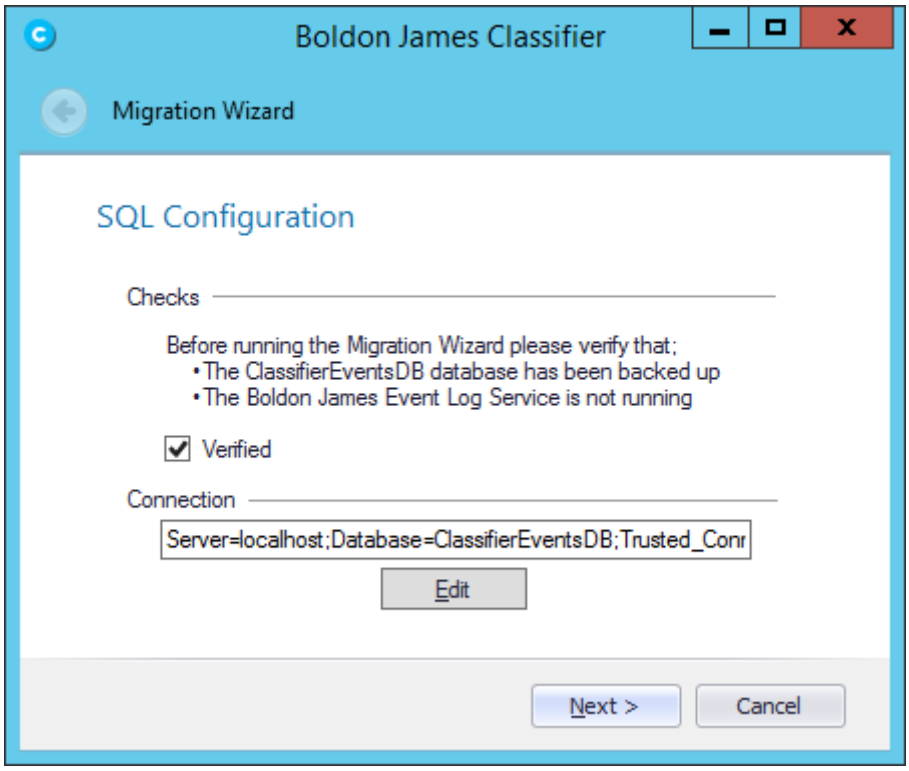
As with the Event Log Service, this application must have access to a published Classifier Configuration so that it can access definitions of labels and policies needed to parse Event labels into individual selector values.

The wizard will write this configuration to the database, and will parse all the current labels and add the results to the appropriate tables and views. Note that the application will not attempt to process any staging data. It is assumed that the staging data will have already been processed.

The wizard has two pages. The first is a configuration page, and the second page has a viewer to report the progress of the conversion.

Page 1

Configure the SQL connection to the server, and verify that the database has been backed up and that the Boldon James event log service is not running.



Migration Wizard Page 1

To configure the connection to the database, press the **Edit** button to show the SQL Connection Editor screen.

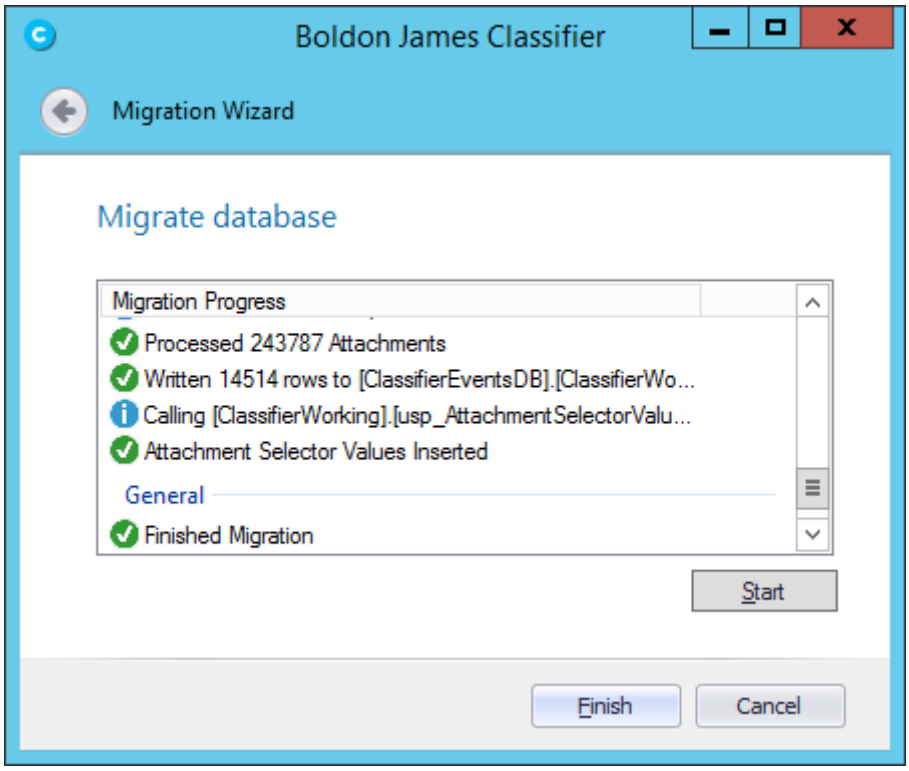
SQL Connection Editor

Enter the name of the server that hosts the database: If you run the migration wizard on the server that hosts the database you can enter "**localhost**". If you have created the Classifier Events database in an instance other than the default instance, you will have to add the name of the

instance to the string, for example "**localhost\instance#1**". The Database must always be **ClassifierEventsDB**. Select either Windows or SQL Server Authentication. The windows account or SQL Server account must be configured in the database with the ***ClassifierSupplierRole***, (see the section on configuring the Event Log Service for details on how to configure an account with the ***ClassifierSupplierRole***). You can test the connection to the database by clicking the **Test**. Once the connection has been configured, you should click the **Next** button to move to the next page.

Page 2

Press the **Start** button to start parsing label. Progress on the label parsing is displayed. You can stop the process by pressing the **Cancel** button. Note, that pressing the **Cancel** button will not roll back the processing, but, if there are any issues the application can be run again as it will re-build the data it adds to the database. When the processing has finished, click the **Finish** button to close the migration wizard.



Migration Wizard Page 2

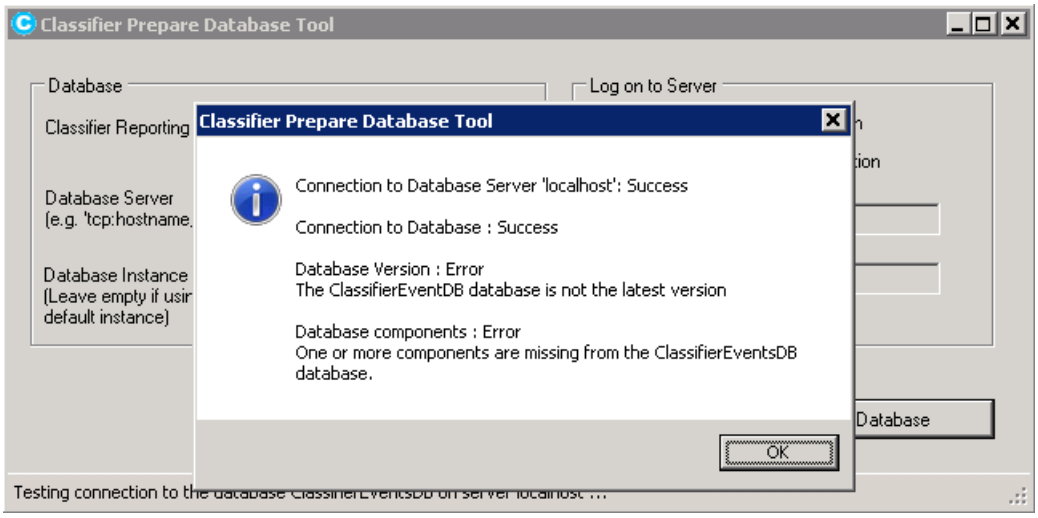
5.2 Updating from a Version 1.2 database to a Version 1.3 database

If you have a version 1.2 database you **must** upgrade the database to version 1.3.0 to use the new features in 1.3.0 such as the new dashboards and reports. It is possible to use version 1.2.0 of the console with a version 1.3.0 database but you will need to upgrade the console to version 1.3.0 to use the new reports and dashboards.

Note: If you have a version 1.0.0 database and you want to upgrade it to a version 1.3.0 database, you will have to upgrade the database to version 1.2.0 first and then upgrade the version 1.2.0 database to version 1.3.0.

You can upgrade a version 1.2.0 database to a version 1.3.0 database by completing the following steps.

1. Stop the SQL Server Agents so that no batch processing of events take place during the update process.
2. Run the new Prepare Database program. Enter the name of the server running the SQL Server database and the appropriate authentication details.
3. Press the ***Test*** button. The following message will be displayed if the Classifier Reporting database needs updating. Close the Prepare Database program.



Database Version Warning

4. At this stage you will need to run a script in **SQL Server Management Studio,** called C:\Program Files (x86)\Boldon James\Classifier Reporting Services\ SQL\ UpdateDatabase.sql to start the update process.

   Note: Updating the database may take some time so you may want to schedule running this script at a time of low database usage. You may also want to perform a database backup before running the script.

5. Once the script has completed, run the Prepare Database program and press the ***Update Database*** button. This runs a set of SQL scripts that will complete the update of the Classifier Reporting Database.

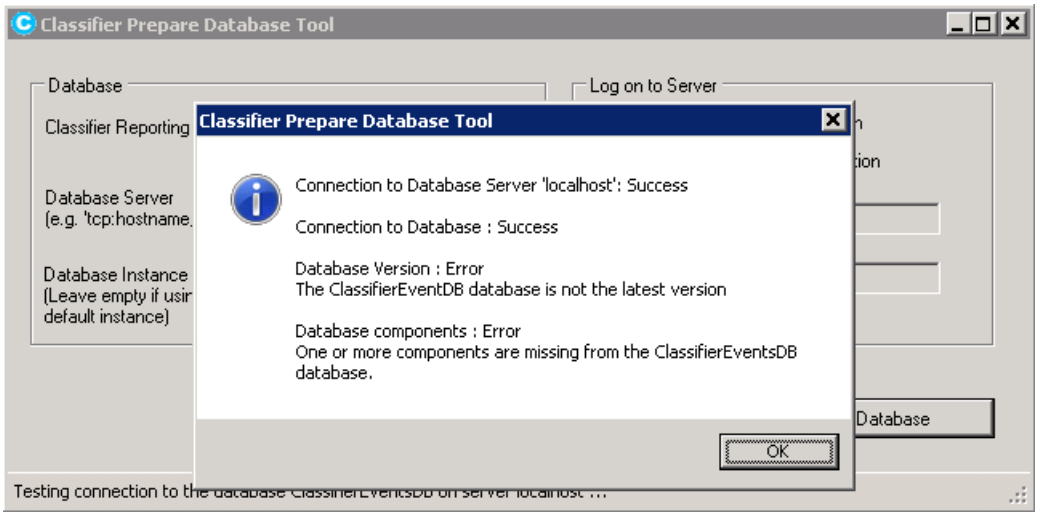
6. When the process is finished, you should test whether the Classifier Reporting Database has been successfully created by pressing the ***Test*** button
7. Restart the SQL Server Agent.
8. The Database Management program creates a text file showing the progress of the creation process. If there is a problem creating the database, you can check the file for details. The file is **C:\Users\<UserName>\AppData\Local\Temp\PrepareDatabase.log**

Note: You do not have to run the Migration Wizard to update from version 1.2 to version 1.3.

5.3 Updating from a Version 1.3.0/1.3.1/1.4.0 database to a Version V1.4.1 database

If you have a version 1.3.0, 1.3.1 or V1.4.1 database, you can upgrade to a V1.4.1 database by completing the following steps.

1. Stop the SQL Server Agents so that no batch processing of events take place during the update process.
2. Run the new Prepare Database program. Enter the name of the server running the SQL Server database and the appropriate authentication details.
3. Press the ***Test*** button. The following message will be displayed if the Classifier Reporting database needs updating.



Database Version Warning

4. Press the ***Update Database*** button. This runs a set of SQL scripts that will complete the update of the Classifier Reporting Database.
5. When the process is finished, you should test whether the Classifier Reporting Database has been successfully upgraded by pressing the ***Test*** button
6. Restart the SQL Server Agent.
7. The Database Management program creates a text file showing the progress of the creation process. If there is a problem creating the database, you can check the file for details. The file is **C:\Users\<UserName>\AppData\Local\Temp\PrepareDatabase.log**

Note: You do not have to run the Migration Wizard to update from version 1.3.0, 1.3.1 or V1.4.0 to version 1.4.1.

6 CONFIGURING THE CLASSIFIER REPORTING SERVICES

6.1 Configuring the Event Log Service

The Event Log Service reads information from the Windows Event log and writes the information into the Classifier Reporting Database. The following information explains how the service should be configured. The service should be run on the system holding the consolidated Classifier event logs.

6.1.1 Configuring the Classifier Policy

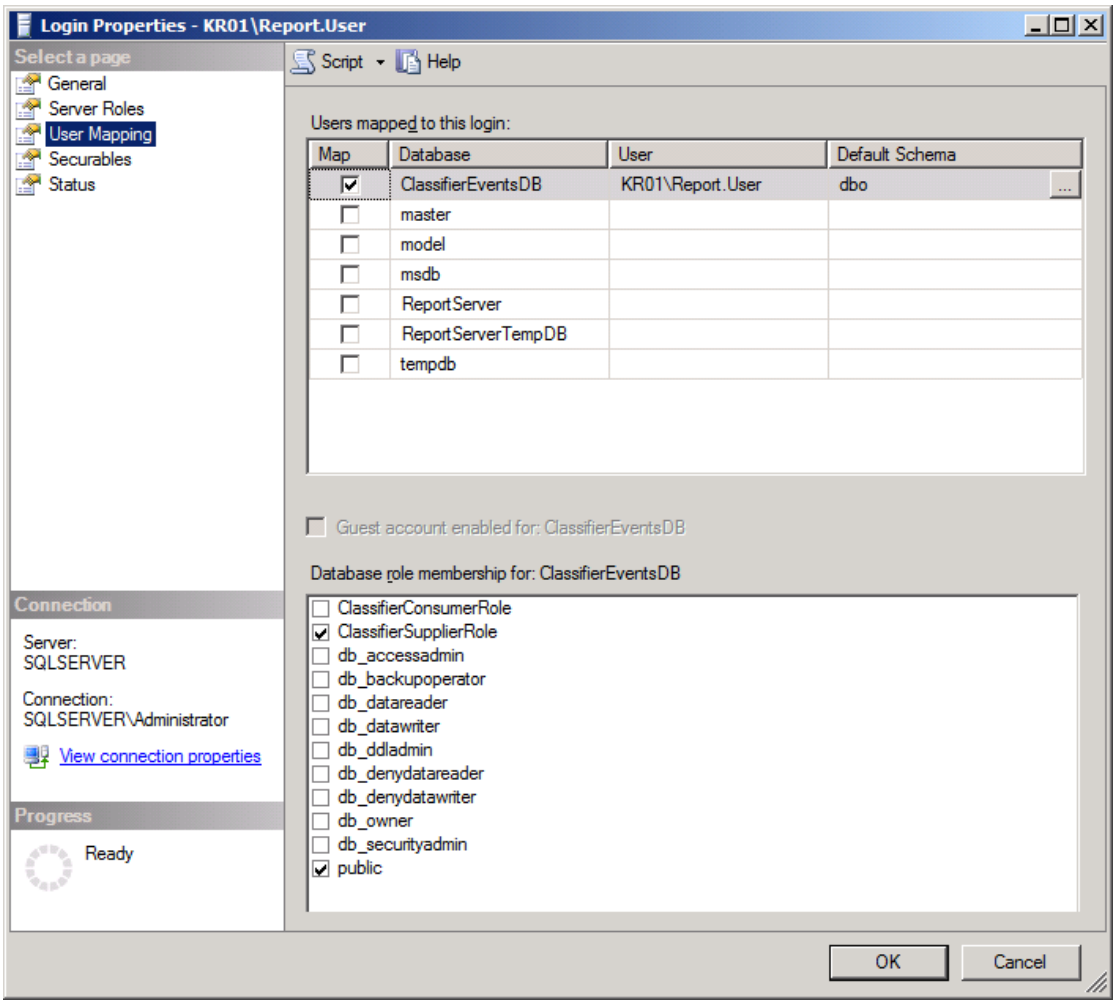
The Event Log Service needs access to a Classifier policy for licensing and label parsing. Configuring access to a policy is explained in more detail in the section Classifier Configuration.

6.1.2 Configuring a Database login

The Event Log Service has to be configured to be run by a login that has access to the Classifier Reporting database. This login can be either based on Windows authentication or SQL Server authentication.

Note: The database instance has to be configured for both SQL Server and Windows Authentication mode if you want to define a login using SQL Server authentication.

1. If you want to use Windows authentication you will need to use a Windows domain account to run the service. This account does not have to be a member of the Domain Admin group but should have read permission to the local event log.
2. First, using **SQL Server Management Studio** create a security login and either associate the login either with a Windows domain account or configure the login to use SQL Server authentication.
3. Secondly, you have to grant permissions to the login to write event data to the database by mapping the account to the ***ClassifierSupplierRole*** as shown below.

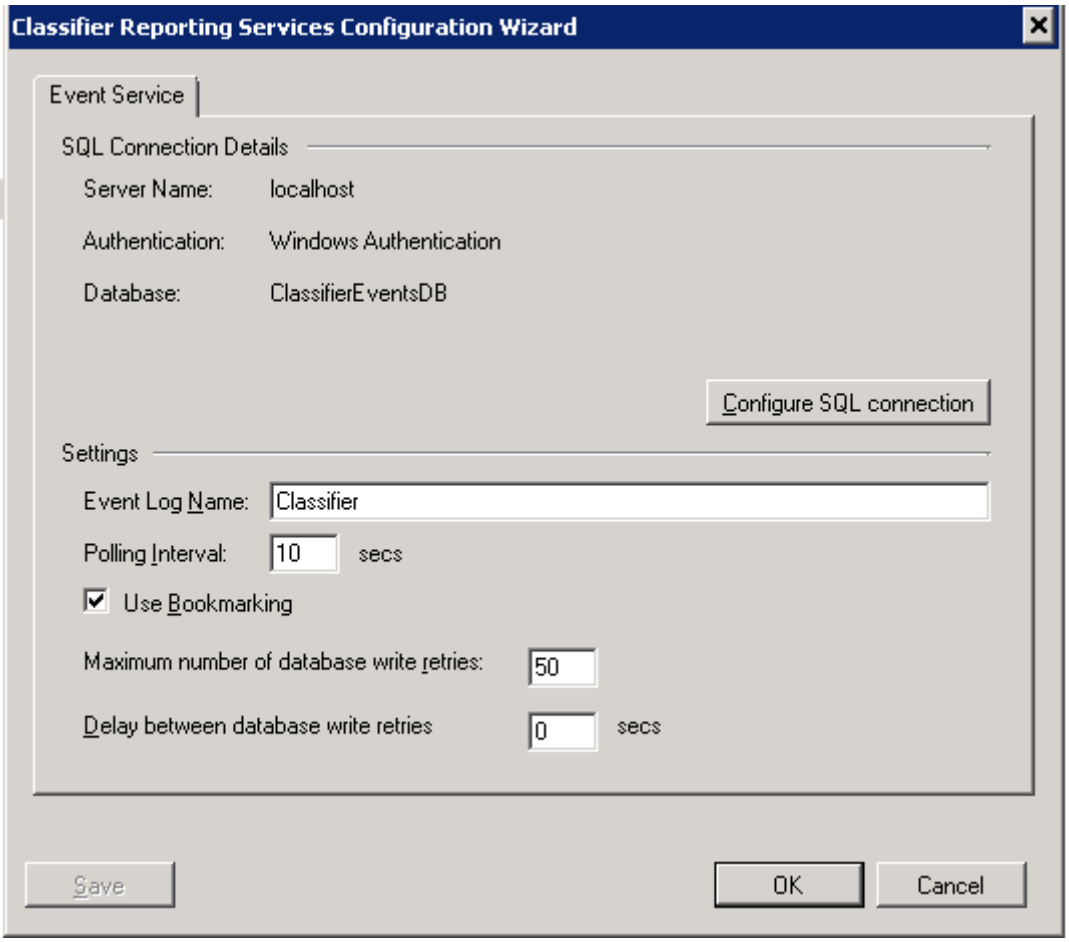


Map login to **ClassifierSupplierRole** role

6.1.3 Configuring the Event Log Service using the Configuration Wizard

Once you have created a database login you should configure the Event Log Service using the Configuration Wizard, see the picture below. This program enables you to configure values that define how the service runs and details of the database that the service should write to.

Note: In Classifier Reporting V1.3 these values were stored in the registry but from V1.4 onwards these values are only stored in the configuration file and are managed using the Configuration Wizard.



Configuration Wizard for the Event Log service.

The fields of the Configuration Wizard will now be explained.

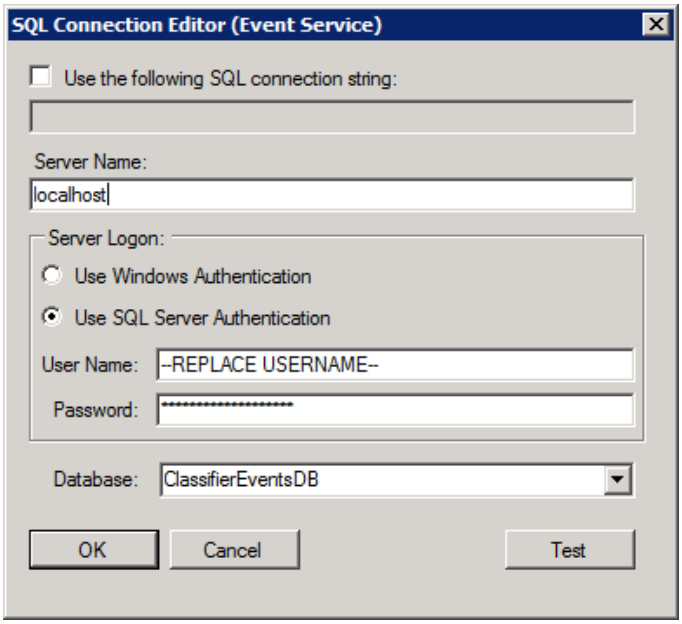
- ***Event Log Name*** is the name of the consolidated event log. If you have followed the event forwarding steps in section 3 above, then this value should be "**Classifier**". Alternatively, if you use the Windows Logs/Forwarded Events event channel the value should be set to "**ForwardedEvents**", note that the value should contain no space characters *(default: Classifier)*.
- ***Polling Interval*** is the number of seconds the service waits to poll the Event Log for new events *(default: 10 seconds)*.
- ***Use Bookmarking*** configures the service to remember the last event it processed, so that every time the service is polled, and if the service is restarted, it will continue processing events from the bookmarked position and not from the start of the Event Log *(default: checked)*.

  Unchecking the ***Use Bookmarking*** option configures the service to process all the events in the Event Log every time the service polls for new events and every time the service is restarted.
- **Maximum number of database write retries** and **Delay between database write retries** are discussed in section on database connection management.
- The ***Save*** button writes configuration data to files.

- The ***OK*** button writes configuration data to files and then closes the Configuration Wizard.
- The ***Cancel*** button exits the Configuration Wizard without saving any configuration data.
- The ***Configure SQL connection*** button displays the SQL Connection Editor dialog as described in the next section.

6.1.4 SQL Connection Editor for the Event Log Service

The SQL Connection Editor is the place where you can define information about the database that the Event Log service will write data to. The Event Log service will use a SQL connection string to connect to the database. You can define this string yourself or let the SQL Connection Editor construct the string with the information you provide.



SQL Connection Editor.

The fields on the SQL Connection Editor will now be explained.

- The ***Use the following SQL Connection String*** option allows you to define your own SQL connection string. See section Defining your own SQL Connection string for more details.
- ***Server Name*** is the name of the server hosting the Classifier Reporting database. If the Event Log Service is being deployed on the same server as the database this name can be left as **localhost**.

  If you have created the Classifier Events database in an instance other than the default instance, you will have to add the name of the instance to the server name. For example, if your database is stored in an instance called myInstance then set the server name to **localhost\myInstance**.

  If your SQL Server is not listening on the default TCP port, you will have to add the port that the SQL Server is listening on to the server name. For example if your SQL Server is available on port 1434, set the server name to **localhost,1434**.

If your SQL Server is stored in an instance called myInstance and is listening on port 1434 then set the server name to **localhost\myInstance,1434**

- ***Use Windows Authentication*** – this configures the service to use the domain account that the service is configured to run as, to authenticate with the SQL Server. See Starting the Event Log Service for more details.
- ***Use SQL Server Authentication*** - this configures the Event Log service to use the SQL Server login and credentials defined in the ***User Name*** and ***Password*** fields. The SQL Server login must be associated with the ClassifierConsumerRole as explained in the Configuring a Database login section.

  In the picture above, for example, replace the text ***–REPLACE USERNAME –*** with the SQL Server login name.
- ***Database*** is the name of Classifier Events database and should always be **ClassifierEventsDB**.
- The ***Test*** button attempts a SQL connection to the database using the provided details.
- The ***OK*** button first attempts a SQL connection to the database using the provided details and if the connection is successful, the details are saved and the SQL connection editor is closed.
- The ***Cancel*** button closes the SQL connection editor without saving any configuration details.

6.1.5 Defining your own SQL Connection string

If the ***Use the following SQL Connection String*** option is selected it is possible to change the SQL Connection string created by the SQL Connection Editor, for example if you want to encrypt the SQL connection between the services and the database you could add the required keywords to the SQL Connection string.

The SQL Connection strings created by the SQL Connection editor have the following format.

- If Windows Authentication is being used, the format is

  Data Source=<Server name>; Initial Catalog=ClassifierEventsDB;Integrated Security=True

  Where ***<Server name>*** is the name of the server hosting the Classifier Reporting database.
- If SQL Server Authentication is being used, the format is

  Data Source=<Server name>; Initial Catalog=ClassifierEventsDB;Integrated Security=False, User ID=<Login Name>,Password=<Password>

  Where ***<Server name>*** is the name of the server hosting the Classifier Reporting database.

  <Login Name> is the name of the SQL Login name created to access the database.

  <Password> is the password of the SQL Login.

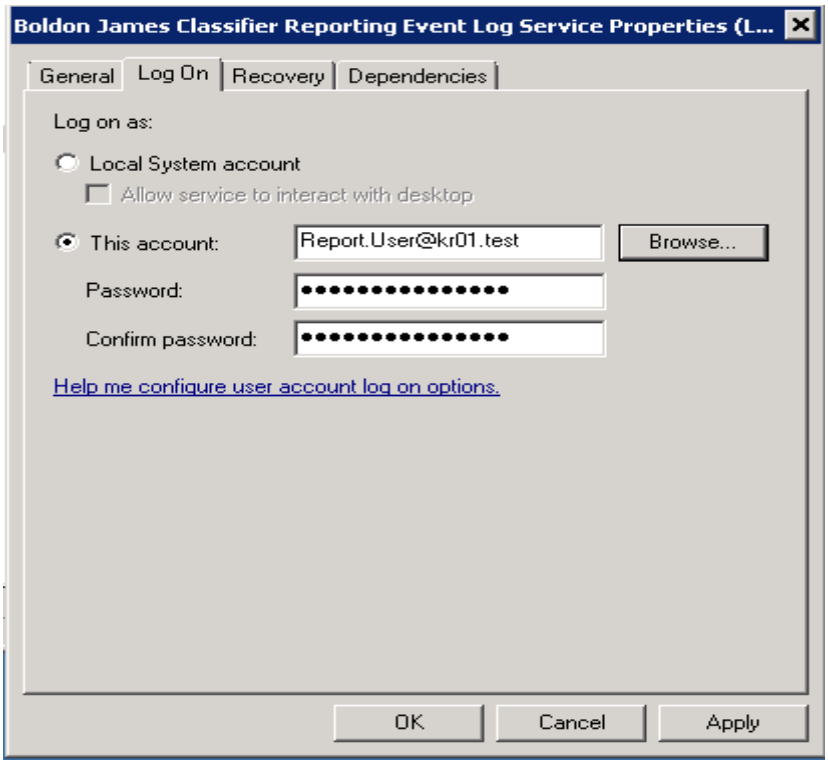
The website https://www.connectionstrings.com/sql-server/ is a good general reference for SQL Connection strings and the website https://docs.microsoft.com/en-us/sql/relational-databases/native-client/applications/using-connection-string-keywords-with-sql-server-native-client?view=sql-server-2017 provides a list of SQL Server SQL Connection string keywords.

Note: If you change the SQL Connection string you should always retain the Initial Catalog=ClassifierEventsDB component.

6.1.6 Starting the Event Log Service

The Event Log service is started from the Services console.

1. You have to create or configure, a Windows domain account to run the service. This account does not have to be a member of the Domain Admin group but should have read permission to the local event log.



Configuring a domain user to run the service

2. If you want to use Windows authentication to access the database, the domain account should be associated with the ClassifierConsumerRole as explained in the Configuring a Database login section.
3. If you want to use SQL Server authentication you still need to configure a Windows domain account to run the service but then you have to use the Configuration Wizard to configure the service to use a SQL Server login to access the database as explained in the Configuring the Event Log Service using the Configuration Wizard section. The SQL Server login must be associated with the ClassifierConsumerRole as explained in the Configuring a Database login section.

Note: If you want to configure the service as Automatic, we recommend configuring the service as 'Delayed start' Automatic.

6.1.7 Database Version Check

When the Event Log Service is started, both as a service and when run from a console, it checks the version of the database and only starts if the database is a compatible version.

6.1.8 Database Connection Management

It's possible that the Event Log Service is temporarily prevented from writing event data into the Classifier Reporting database because the database's batch processes are running and have locked other processes from accessing the database. It this case the Event Log Service can be configured to re-try writing the event. This process is controlled by the following two parameters

Maximum number of database write retries is the maximum number of times the Event Log Service will try to write the event to the database before waiting a number of seconds before re-trying to write the event again. The number of seconds the Event Log Service will wait is set by **Delay between database write retries.**

For example, if **Maximum number of database write retries** is set to 10 and **Delay between database write retries** is set to 30, the Event Log Service will try to write the event to the database 10 times. If it is unsuccessful, the Service will wait 30 seconds and then re-try another 10 times. This sequence will continue until the event is finally written to the database.

If **Delay between database write retries** is set to 0 or is not set, the Event Log Service will make up to **Maximum number of database write retries** attempts to write an event to the database. If the Event Log Service still can't write the event after re-trying **Maximum number of database write retries** times the event will be discarded and the Event Log Service will attempt to write the next event.

6.2 Configuring the AD Service

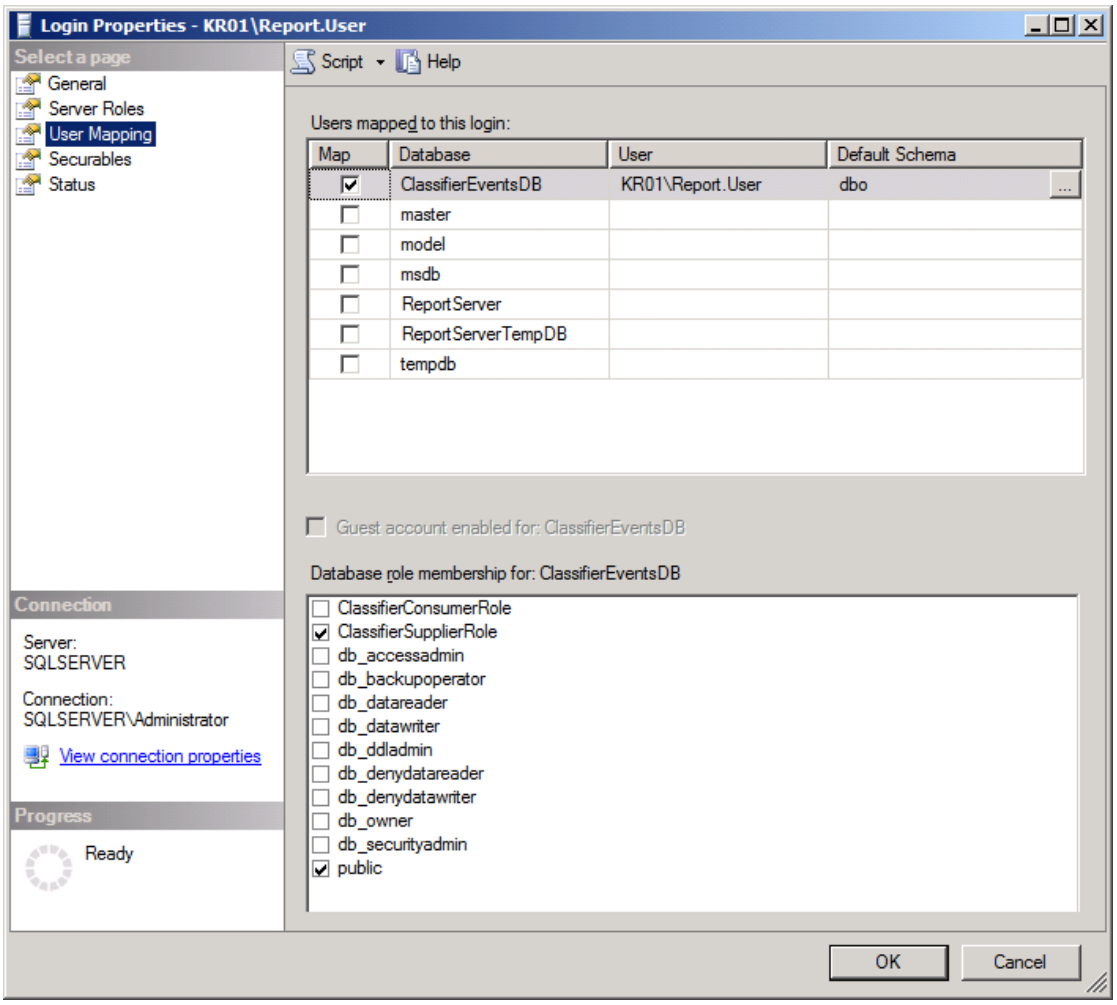
The AD Service reads information about Users and Computers from the Active Directory and writes the information to the Classifier Reporting Database to provide supplementary information for use in the Reports generated. The following information explains how the service should be configured.

6.2.1 Configuring a Database login

The AD Service has to be configured to be run by a login that has access to the Classifier Reporting database. This login can be either be based on Windows authentication or a SQL Server authentication.

Note: The database instance has to be configured for both SQL Server and Windows Authentication mode if you want to define a login using SQL Server authentication.

1. If you want to use Windows authentication you will need to use a Windows domain account to run the service. This account does not have to be a member of the Domain Admin group but does require read permissions for the Active Directory to read non-deleted items in the Directory but the account does have to be a member of the Domain Admin group if you wish to read details of items that have been deleted from the Directory.
2. First, using **SQL Server Management Studio** create a Security login and either associate the login either with a Windows domain account or configure the login to use SQL Server authentication.
3. Secondly, you have to grant permissions to the login to write event data to the database by mapping the account to the ***ClassifierSupplierRole*** as shown below.

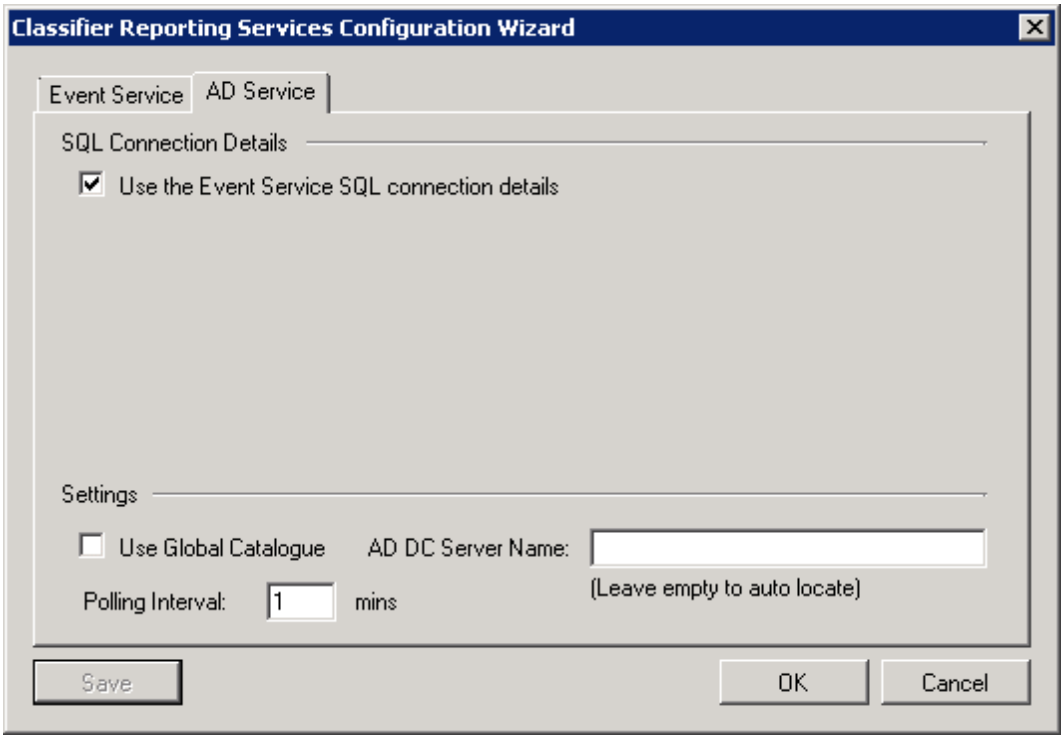


Map login to **ClassifierSupplierRole** role

6.2.2 Configuring the AD Service using the Configuration Wizard

Once you have created a database login you should configure the AD Service using the Configuration Wizard, see the picture below. This program enables you to configure values that define how the service runs and details of the database that the service should write to.

Note: In Classifier Reporting V1.3 these values were stored in the registry but from V1.4 onwards these values are only stored in the configuration file and are managed using the Configuration Wizard.



Configuration Wizard for the AD service using Event Log service connection details.

The fields of the Configuration Wizard will now be explained.

- ***Use the Event Service SQL connection details*** – when this option is selected, the AD Service will use the same SQL connection details as configured for the Event Service, see the section Configuring the Event Log Service using the Configuration Wizard.
- ***Use Global Catalogue*** configures the AD Service to use the Active Directory Global Catalogue to read users and computers attributes. Select this option if your organisation has an Active Directory Forest of Domains and you wish to read information about all users and computers in all your organisation's domains. Don't select this option if you only have one domain or only wish to read information from your local domain.

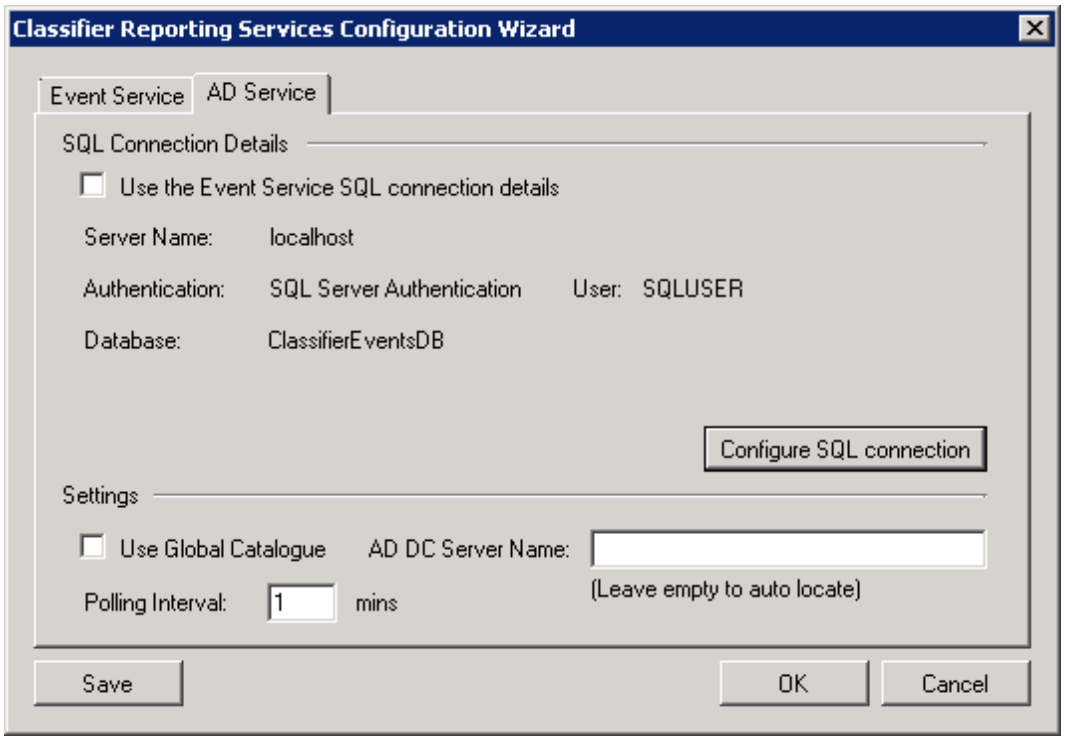
  Note: When connecting to the Global Catalogue, the AD service will only copy to the database the user and computer AD attributes that are replicated to the Global Catalogue.

- ***AD DC Server Name***, the name of the computer that holds the Active Directory (AD). If this value is not set, the AD service will automatically locate the Domain Controller. ***This value is ignored if Global Catalogue is used***.
- ***Polling Interval*** is the length of time in minutes that the service waits before checking for changes in the Users and Computers AD containers *(default 1 minute)*.
- The ***Save*** button writes configuration details to the configuration file.

- The ***OK*** writes configuration details to the configuration file and then closes the Configuration Wizard.

- The ***Cancel*** button closes the Configuration Wizard without saving the configuration details.

If the ***Use the Event Service SQL connection details*** option is not set, the Configuration Wizard will look as shown below.



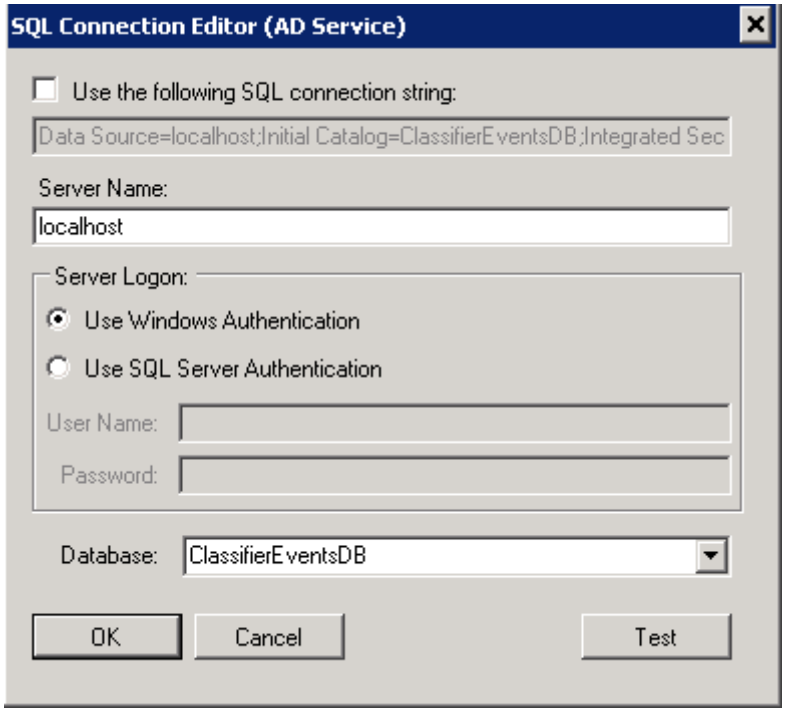
Configuration Wizard for the AD service not using Event Log service connection details.

There is one additional field to explain.

- The ***Configure SQL connection*** button displays the SQL Connection Editor dialog as described in the next section.

6.2.3 SQL Connection Editor for the AD Service

The SQL Connection Editor is the place where you can define information about the database that the AD service will write data to. The AD service will use a SQL connection string to connect to the database. You can define this string yourself or let the SQL Connection Editor construct the string with the information you provide.



SQL Connection Editor for the AD service

The fields on the SQL Connection Editor will now be explained.

- The ***Use the following SQL Connection String*** option allows you to define your own SQL connection string. See the section Defining your own SQL Connection string for more details.
- ***Server Name*** is the name of the server hosting the Classifier Reporting database. If the AD Service is being deployed on the same server as the database this name can be left as **localhost**.

  If you have created the Classifier Events database in an instance other than the default instance, you will have to add the name of the instance to the server name. For example, if your database is stored in an instance called myInstance then set the server name to **localhost\myInstance**.

  If your SQL Server is not listening on the default TCP port, you will have to add the port that the SQL Server is listening on to the server name. For example if your SQL Server is available on port 1434, set the server name to **localhost,1434**.

  If your SQL Server is stored in an instance called myInstance and is listening on port 1434 then set the server name to **localhost\myInstance,1434**
- ***Use Windows Authentication*** – this configures the AD Service to use the domain account that the Service is configured to run as, to authenticate with the SQL Server. See Starting the AD Service for more details.
- ***Use SQL Server Authentication*** - this configures the service to use the SQL Server login and credentials defined in the ***User Name*** and ***Password*** fields. The SQL Server login must be associated with the ClassifierConsumerRole as explained in the Configuring a Database login section.

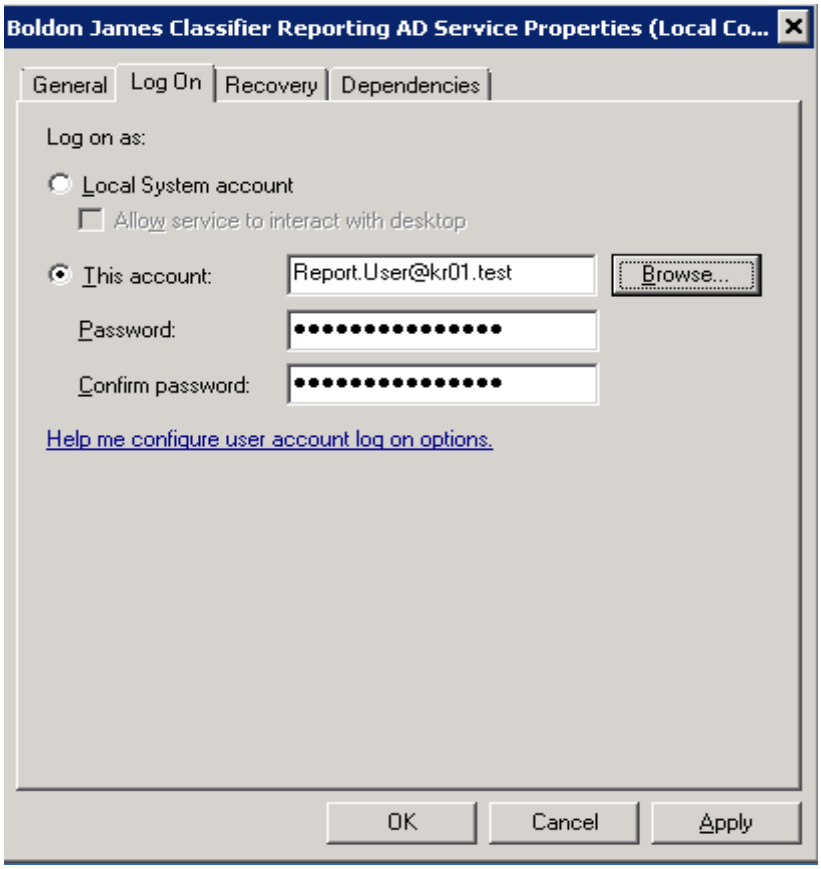
In the picture above, for example, replace the text ***–REPLACE USERNAME –*** with the SQL Server login name.

- ***Database*** is the name of Classifier Events database and should always be **ClassifierEventsDB**.
- The ***Test*** button attempts a SQL connection to the database using the provided details.
- The ***OK*** button first attempts a SQL connection to the database using the provided details and if the connection is successful, the details are saved and the SQL connection editor is closed.
- The ***Cancel*** button closes the SQL connection editor without saving any configuration details.

6.2.4 Starting the AD Service

The AD service is started from the Services console.

1. You have to create or configure, a Windows domain account to run the service. This account does not have to be a member of the Domain Admin group but does require read permissions for the Active Directory to read non-deleted items in the Directory but the account does have to be a member of the Domain Admin group if you wish to read details of items that have been deleted from the Directory.



Configuring a domain user to run the AD service

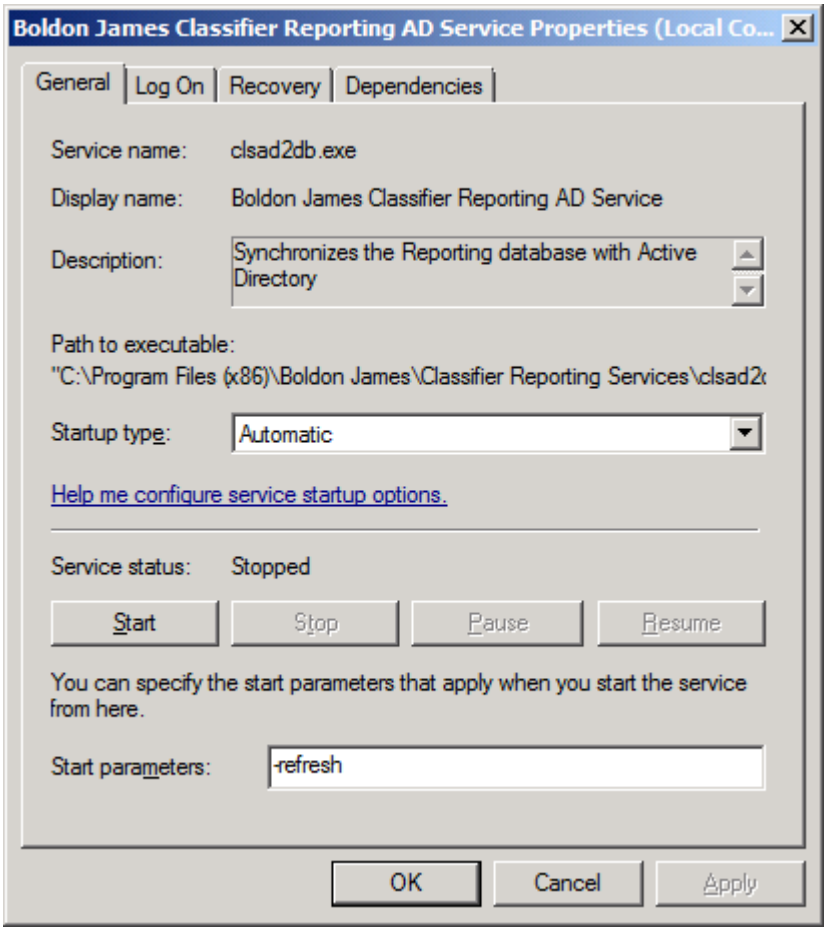
2. If you want to use Windows authentication to access the database, the domain account should be associated with the ClassifierConsumerRole as explained in the Configuring a Database login section.
3. If you want to use SQL Server authentication you still need to configure a Windows domain account to run the service but then you have to use the Configuration Wizard to configure the service to use a SQL Server login to access the database as explained in the Configuring the AD Service using the Configuration Wizard section. The SQL Server login must be associated with the ClassifierConsumerRole as explained in the Configuring a Database login section.

Note: If you want to configure the service as Automatic, we recommend configuring the service as 'Delayed start' Automatic.

6.2.5 Forcing a AD data refresh

The AD Service reads user and computer information from the Active Directory the first time it is run. The AD service then periodically checks for updates in the user and computer information at a time interval determined by the **PollTimeInMinutes** setting, see above. The AD service will continue to check for updates even if it is restarted. The service uses a cookie, stored on the local system, to record what user and computer items have been read from the Active Directory.

However, it is possible to force the AD service to re-read all the users and computer information, not just updates, when it is restarted by specifying "Start parameters" of **–refresh** as shown below.



AD service configured to re-read all user and computer information.

6.2.6 Computer and User AD attributes

This feature allows the administrator to define which AD attributes on the AD Computer and User objects should be retrieved from AD and written to the SQL database when the AD Service polls for changes.

Upto 10 attributes can be defined for retrieval for both Computer and User objects – these values are written into columns labelled “*Attribute1*” to “*Attribute10*” in the “*Computers*” and “*KnownUsers*” tables.

The attributes to be retrieved are defined in the AD Service configuration file “clsad2db.exe.config” located in the installation directory (default: C:\Program Files (x86)\Boldon James\Classifier Reporting Services). See 9.2.2 below for details.

7 DATABASE FEATURES

7.1 Security Considerations

7.1.1 Database Roles

Security in the Classifier Reporting Database is enforced by using the following three SQL Server database roles.

ClassifierSupplierRole. Logins mapped to the ClassifierSupplierRole are granted EXECUTE permission to use stored procedures that write data into the Staging tables. The role is intended to be used by the Event Log Service and the AD Service. See the sections Configuring the Event Log Service and Configuring the AD Service for more details.

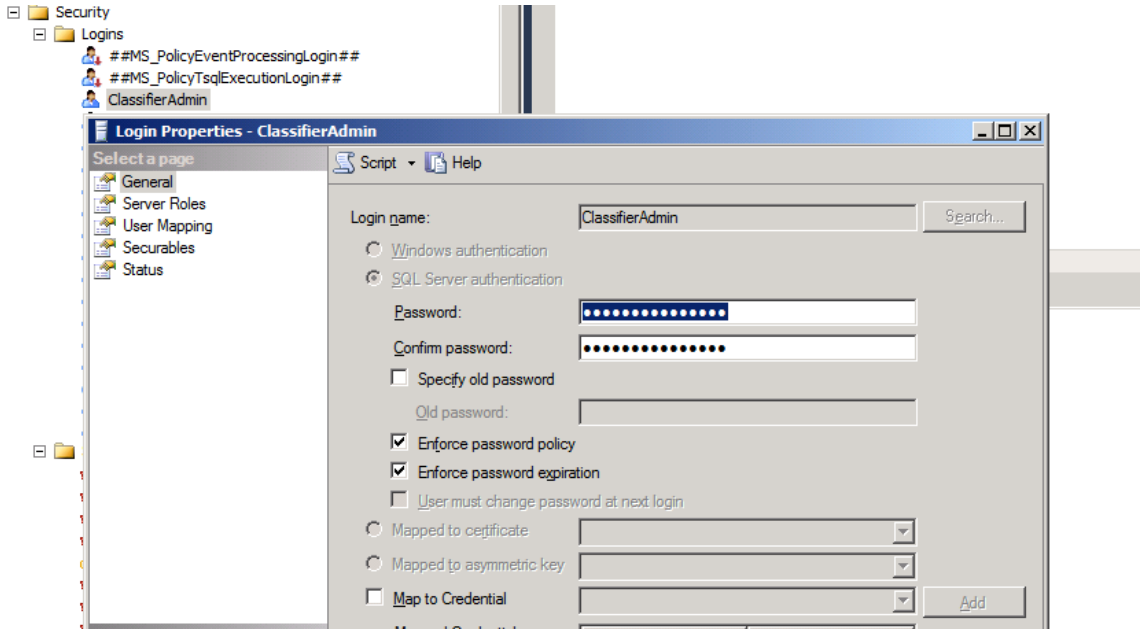
ClassifierConsumerRole. Logins mapped to the ClassifierConsumerRole are granted SELECT permission on the view schemas. The role is intended to be used by Users that run the Console to create dashboards and reports. Further information can be found in the **Classifier Reporting Console Guide (UM6422).**

ClassifierMaskedConsumerRole. Logins mapped to the ClassifierMaskedConsumerRole are granted SELECT permission on the view schemas but do not have access to masked columns. The role is intended to be used by Users that run the Console to create dashboards and reports but do not have the privileges to view information that could identify individual people or computers. Further information can be found in the **Classifier Reporting Console Guide (UM6422).**

ClassifierMaintenanceRole. Logins mapped to this role are granted EXECUTE and ALTER permissions to run the stored procedures that transfer data between the Staging and Working tables. When the database is created A User called ***ClassifierAdminUser*** is created and mapped to the ClassifierMaintenanceRole. This User is associated with a Login called ***ClassifierAdmin*** that then has the permissions to run the SQL jobs that run the stored procedures to transfer data between the Staging and Working tables and can create table indices.

7.1.2 Changing *ClassifierAdmin* password

When the Classifier Reporting Database is created a password is assigned to the ***ClassifierAdmin*** Logon by the installation program. **It is strongly recommended that this password is changed by the SQL System Administrator** as shown below:



Change Password

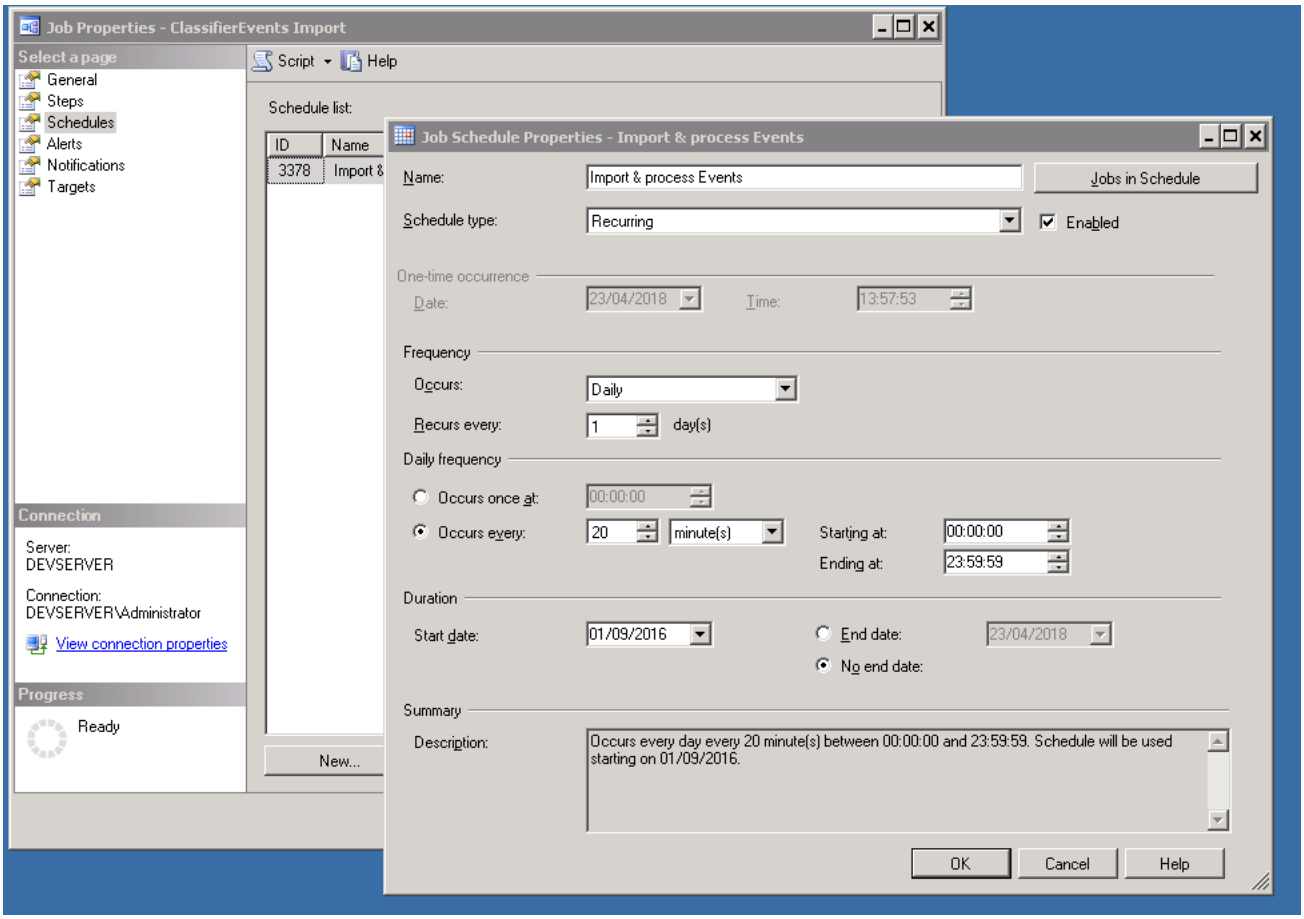
7.2 Automatic Event Processing and Deletion

The Classifier Reporting Services makes use of SQL jobs to process event information into a form suitable for the Classifier Reporting Console. To perform this processing automatically the SQL Server Agent Windows Service must be running. The following article explains how to do this.

http://www.mssqltips.com/sqlservertip/2729/how-to-start-sql-server-agent-when-agent-xps-show-disabled/

7.2.1 ClassifierEvents Import

The **ClassifierEvents Import** job runs the stored procedures to convert event data from the Staging to Working tables and to create the tables used by the Classifier Reporting Console. It is scheduled to run every 20 minutes but it is possible to change the schedule and run the SQL job more or less frequently.



Changing Job Schedule Properties

7.2.2 AD Data Import

The **AD Data Import** job calls stored procedures to convert User and Computer data, read from the Active Directory, from the Staging to Working tables. It is scheduled to run every 10 minutes but it is possible to change the schedule and run the SQL job more or less frequently.

7.2.3 ClassifierEvents Delete

The ClassifierEvents Delete job calls a stored procedure to delete data from the Working tables that are older than a configured number of months. After installation this period is set to 6 months but this can be changed by setting the following value in the Classifier Reporting Database.

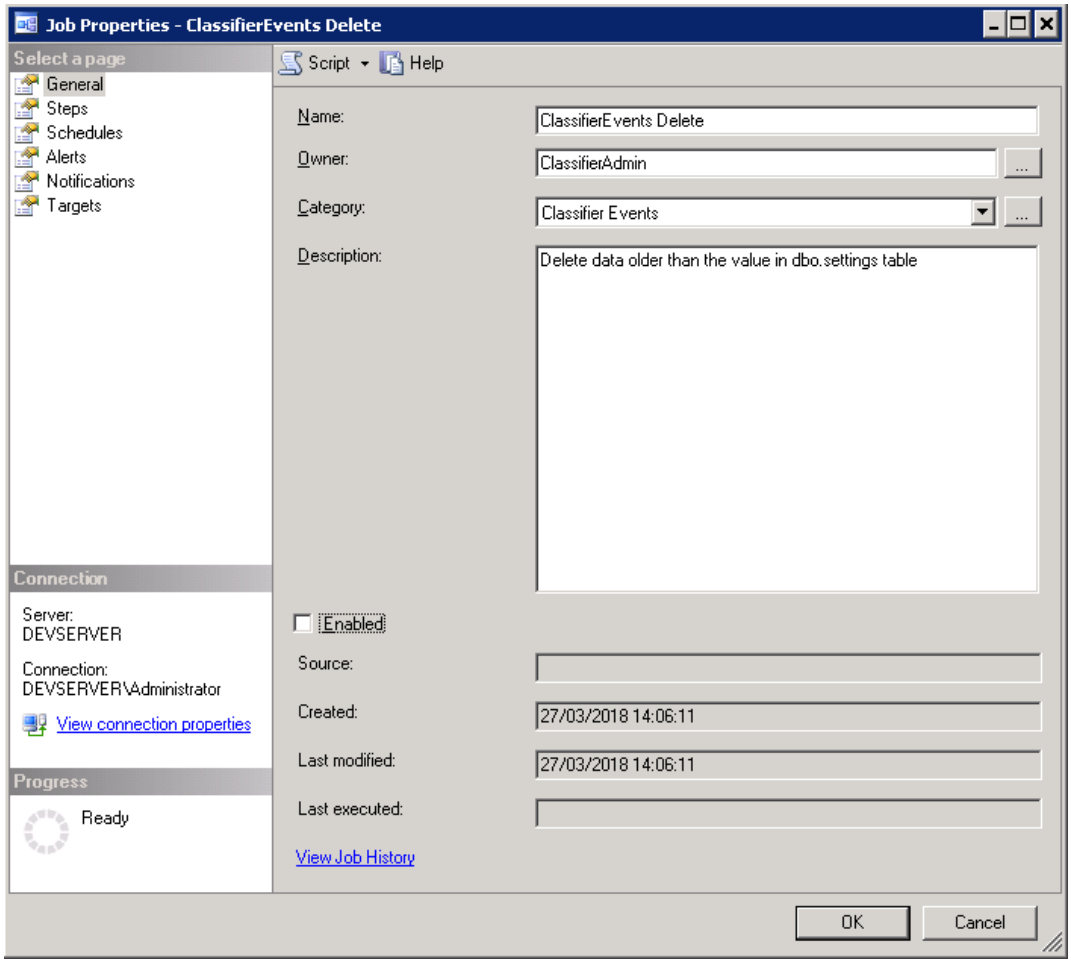
Table	Row	Column	Value
[ClassifierEventsDB].[dbo].[Settings]	SettingId=1	SettingValue	Number of months

For example, to change this value, to say every 2 months, run the following SQL statements in **SQL Server Management Studio**

use ClassifierEventsDB

update ClassifierEventsDB.dbo.Settings set SettingValue=2 where SettingId=1

The SQL job is scheduled to run once a day but the SQL job is disabled after installation. The SQL job can be enabled by setting the **Enabled** check box as shown below.



Enabling the ClassifierEvents Delete SQL job.

7.3 Indexes

A set of indices can be added to the Classifier Reporting Database to improve the performance of Event processing and SQL queries performed by the Classifier Reporting Console. The indices are created by a stored procedure called **usp_CreateIndices**. Another stored procedure, called **usp_ReorganizeIndices** checks how fragmented the indices are and reorganises or rebuilds indices that have become too fragmented. The two stored procedures are run by a SQL job called **Index creation and reorganizing**.

7.3.1 Index creation and reorganizing

The **Index creation and reorganizing** job is scheduled to run once every 24 hours. When the job runs it performs the following two steps

Step 1 - Runs the **usp_CreateIndices** stored procedure. When this stored procedure is run for the first time it creates the indices and sets the following field in the database to indicate that the indices have been created.

Table	Row	Column	Value

[ClassifierEventsDB].[dbo].[Settings]	SettingId=3	SettingValue	1, implies indices have been created.

When the procedure is run again by the SQL job it checks if the database field has been set and if it has, does nothing. If you want to re-create the indices or if you want to add your own indices to the procedure you should clear the database field by running the following SQL statements in **SQL Server Management Studio**

use ClassifierEventsDB

update ClassifierEventsDB.dbo.Settings set SettingValue=0 where SettingId=3

So that the next time the stored procedure is run the indices will be (re-)created.

Step 2 - Runs the **usp_ReorganizeIndices** stored procedure to defragment the indices.

This will de-fragment the indices. It is possible to change how frequently the job is run. For example if you think that the indexes in your database need defragmenting once every hour you can change the job's schedule properties in **SQL Server Management Studio** as shown below

Note: If you do not want to create any indexes you can disable and/or remove the job after creating the database.

7.4 Data Masking.

The Classifier Reporting Database uses the SQL Server feature Dynamic Data Masking to prevent access, by non-privileged Users, to data that can identify individual people and computers. A list of masked columns in provided in the **Reporting System Database Schema (UM6434)**. To use data masking, Users of the **Classifier Reporting Console** should be mapped to the **ClassifierMaskedConsumerRole**.

Note: Data masking is only provided if the version of SQL Server you are using supports Dynamic Data Masking (See https://msdn.microsoft.com/en-us/library/mt130841.aspx for more details.

8 ADDITIONAL CONSIDERATIONS

8.1 Size of the Classifier Events Database

When planning for your Classifier Events Database it is vital to understand how much disk space will be needed. This depends on many factors including;

- The number of Users in your organisation.
- Which Classifier applications are deployed in your organisation?
- How much information is in each event including the size of file paths and email addresses?
- How long you retain events in the database, see section ClassifierEvents Delete.

8.1.1 Disk space per event.

The Events in the Classifier Reporting Database are processed into a form suitable for creating reports. This creates an amount of overhead in the amount of disk space required for a database but the amount of overhead per-event decreases as the number of Events stored in the database increases. Based on empirical observations a database of 10 million entries, will take about **3229 bytes** per event.

8.1.2 Calculating the amount of disk space required

In a typical organisation, how much disk space would be needed?

Consider the following

- Number of Users = Nu
- Number of Events per day = Nd
- Number of Weeks = Nw

The number of events created in such an organisation is

Ne = Nu * Nd * 5 * Nw

For example, consider an organisation with 1000 Users that generated, on average 50 events per day each. The total number of events for a six-month period would be

Ne = 1000 * 50 * 5 * 26 = 6,500,000.

Assume, from section 4.5.1 every event uses 3229 bytes, 6,500,000 events would therefore require 3229 * 6,500,000 = 20,988,500,000 bytes of disk space, which is approximately 19.5 Gb.

8.1.3 Transaction Log

As well as estimating the disk space needed for the database don't forget that disk space will also be needed for the transaction log and the tempdb database used by SQL Server for temporary storage. When performing procedures such as rebuilding indexes the transaction log can grow to a similar size to the database itself.

The amount of disk space used by the transaction log is also determined by the transaction recovery model. The Classifier Events Database is created using the Full recovery model but this can be changed at any time to suit your environment. Regular backups and compression techniques can be used to reduce the size of the database and the transaction log.

8.2 Other SQL Scripts

The Classifier Reporting Services includes two useful SQL scripts that can be run in **SQL Server Management Studio**. The scripts can be found in ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services\SQL*** directory of the installation disk.

NumberOfRows.sql

This script shows the number of entries in all tables of the Classifier Events Database.

DeleteAll.sql

This script will delete all Event and Active Directory Information from the Classifier Events Database. In effect, leaving the database in the same state as it is after being created. Use with care!

UpdateDatabase.sql

This script converts all the date/time columns in the database from the SQL type DATATIME to SQL type DATETIME2 to increase the precision of times stored in the database. The script also converts several of the table identifier columns from the SQL type INT to SQL type BIGINT to increase the number of events that can be stored in the database. This script is run by **PrepareDatabase** when updating the database from version 1.2 to version 1.3.

RemoveDuplicates.sql

This script contains a set of procedures that can remove duplicate event from the database. See the section Removing duplicate copies of events for more details.

8.3 Removing duplicate copies of events

It is possible that the Classifier Events Database erroneously contains multiple copies of the same events. This could happen, for example, if there are errors in the collection process. Events are considered to be identical if all the fields in the event, including the time created field, are identical.

The SQL script **RemoveDuplicates.sql** contains the following scripts that can be used to remove the unwanted additional copies of events. The script can be found in ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services\SQL*** directory of the installation disk.

ClassifierStaging.usp_RemoveStagingDocumentDuplicates: removes additional copies of events from the ClassifierStaging.StagedDocumentEvents table.

ClassifierStaging.usp_RemoveStagingEmailDuplicates removes additional copies of events from the ClassifierStaging.StagedEmailEvents table.

ClassifierStaging.usp_RemoveStagingMADuplicates removes additional copies of events from the ClassifierStaging.StagedManagementEvents table.

ClassifierStaging.usp_RemoveWorkingDuplicates removes additional copies of events from the ClassifierWorking tables.

Note: The time fields of events before version 1.2.6 were stored in the SQL Server DATETIME format. This format has less precision than the times in the events so times in the database are truncated. Version 1.2.6 now uses the DATETIME2 format so there is no loss of precision in database time columns in events collected by Version 1.2.6 onwards.

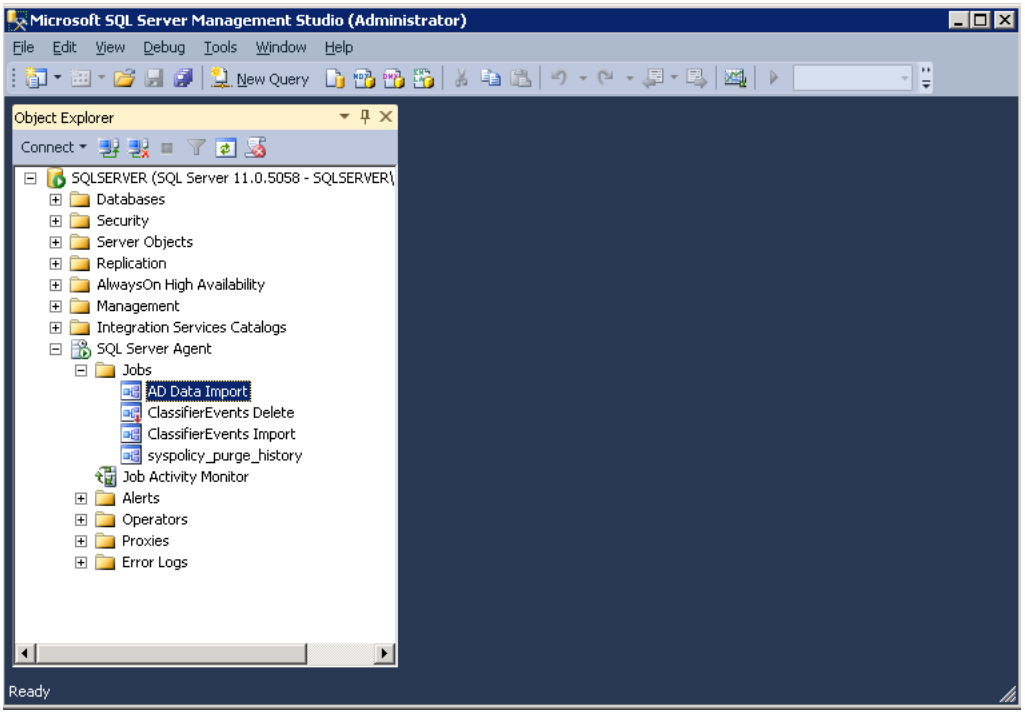
It is possible therefore that events that look identical are in fact distinct events that differ by an extremely small time margin.

Generally there should be no need to use these procedures. If you do observe multiple copies of the same events it is strongly recommended that you review your event collection system and use these procedures as a last resort.

8.4 Removing the Classifier Events Database

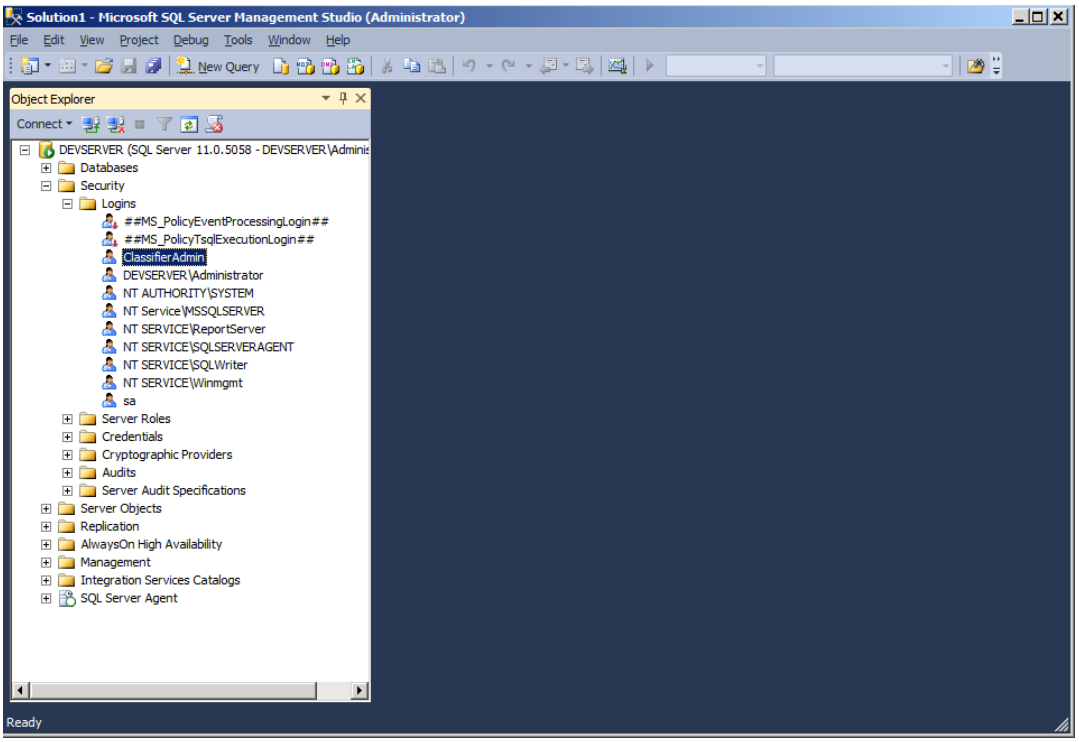
You can remove the Classifier Events Database from your SQL Server by performing the following steps.

1. Stop the Reporting Event Log Service and the Reporting AD Service.
2. Disconnect all Classifier Reporting Console programs from the Classifier Events Database.
3. Remove all the SQL jobs (see section Automatic Event Processing and Deletion) by running **SQL Server Management Studio** and on the tree in the left-hand pane, select **SQL Server Agent->Jobs.**



SQL Server Agent

4. For each of the following **Jobs,** choose **Stop Job** from the context menu. When the job has stopped, choose **Delete** from the context menu.
    - AD Data Import
    - ClassifierEvents Delete
    - ClassifierEvents Import
    - Index creation and reorganising
5. Remove the **Classifier Admin** SQL Login by selecting **Security->Logins** from the tree on the left-hand pane of **SQL Server Management**



SQL Server Agent

6. Select **ClassifierAdmin** and choose **Delete** from the context menu.
7. Remove the Classifier Reports database by selecting **Databases->ClassifierEventsDB,** and choose **Delete** from the context menu.

9 APPENDIX

9.1 Event Log Service configuration file

If the Event Log Service has been installed, the installation directory (typically "C:\Program Files (x86)\Boldon James\Classifier Reporting Services") should contain a configuration file, "**clsev2db.exe.config**". This contains the following settings:

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services***clsev2db.exe.config***		
Property	**Description**	**Default Value**
CustomConnection	Used by the Configuration Wizard to indicate that the SQL connection string has been manually entered.	False
DelayBetweenRetries	Delay in seconds between each batch of [*MaxRetries*] attempts of the Event Log Service at writing a record to the SQL DB. When this value is set to 0 (default) the Event Log Service will give up attempting to write a record to the SQL DB after [*MaxRetries*] attempts.	0
EventLogName	Name of the consolidated event log. If you have followed the event forwarding steps in section 3 above, then this value should be "**Classifier**". Alternatively, if you use the **Windows Logs/Forwarded Events** event channel the value should be set to "**ForwardedEvents**", note that the value should contain no space characters.	Classifier
MaxRetries	The maximum number of times the Event Log Service should attempt to write a record to the SQL DB before giving up. Also see DelayBetweenRetries above.	50
PollingInterval	Number of seconds the service waits to poll the Event Log for new events.	10
SqlConnection	SQL Connection string to the SQL server. Note that if the Configuration Wizard has been used to setup SQL Server Authentication, the SQL connection string will be encrypted. • You may need to amend the Server value but if the SQL Server and Windows Service are co-located then leave this as "localhost". If you have created the Classifier Reporting database in an instance other than the default instance, you will have to add the name of the instance to the string, for example if your database is stored in an instance called myInstance then set the Server value to Server=localhost\myInstance. • If your SQL Server is not listening on the default TCP port you will have to add the port that SQL Server is listening on, to the Server value, for example if your SQL Server is listening on port 1434, set the Server value to Server=localhost,1434.	

	• If your SQL Server is stored in an instance called myInstance and is listening on port 1434 then set the Server value to Server=localhost\myInstance,1434. • The “Database” value must always be “ClassifierEventsDB” • “Trusted_Connection=true” means that the account running the Windows Service will be used to authenticate to SQL Server • If you need to use SQL authentication, then use a SQLConnection string as below where <USERID> is a database login with SQL authentication <add key="SqlConnection" value="Server=<SERVERNAME>; Database=ClassifierEventsDB; User Id=<USERID>; Password=<PASSWORD>;" />	
UseBookmarking	This configures the service to remember (bookmark) the last event it processes so when the process checks for new events, and if the service is stopped and restarted, it processes events from the bookmark i.e. the last event it processed, not from the start of the Event Log. Setting “UseBookMarking” to False configures the service to process all the events in the Event Log every time it polls for new events and every time it is restarted.	True
EventLogConfiguration	This section contains a set of application GUIDs that informs the service which events it should process.	

9.2 Active Directory Service configuration file

If the AD Service has been installed, the installation directory (typically “C:\Program Files (x86)\Boldon James\Classifier Reporting Services”) should contain a configuration file, “**clsad2db.exe.config**”. This contains the following settings:

9.2.1 appSettings Section:

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services***clsad2db.exe.config***		
Property	**Description**	**Default Value**
CustomConnection	Used by the Configuration Wizard to indicate that the SQL connection string has been manually entered.	False
PollTimeInMinutes	Length of time in minutes that the service waits before checking Active Directory (AD) for changes to the Users and Computers containers.	10
ServerName	Name of the Domain Controller (DC) computer that holds the Active Directory (AD). If this value is not set, the AD service will automatically locate the DC. ***This value is ignored if the Global Catalog is used (UseGlobalCatalogue = True).***	

SqlConnection	SQL Connection string to the SQL server. Note that if the Configuration Wizard has been used to setup SQL Server Authentication, the SQL connection string will be encrypted. • You may need to amend the Server value but if the SQL Server and Windows Service are co-located then leave this as “localhost”. If you have created the Classifier Reporting database in an instance other than the default instance, you will have to add the name of the instance to the string, for example if your database is stored in an instance called myInstance then set the Server value to Server=localhost\myInstance. • If your SQL Server is not listening on the default TCP port you will have to add the port that SQL Server is listening on, to the Server value, for example if your SQL Server is listening on port 1434, set the Server value to Server=localhost,1434. • If your SQL Server is stored in an instance called myInstance and is listening on port 1434 then set the Server value to Server=localhost\myInstance,1434. • The “Database” value must always be “ClassifierEventsDB” • “Trusted_Connection=true” means that the account running the Windows Service will be used to authenticate to SQL Server • If you need to use SQL authentication, then use a SQLConnection string as below where <USERID> is a database login with SQL authentication <add key="SqlConnection" value="Server=<SERVERNAME>; Database=ClassifierEventsDB; User Id=<USERID>; Password=<PASSWORD>;" />	
UseGlobalCatalogue	Use Global Catalogue. Determines whether the AD service uses the Global Catalog (GC) to read Users and Computers information. Set this to “***True***” if your organisation has an AD Forest of Domains and you wish to read information about all Users and Computers in all your organisations domains. Set this to “***False***” if you only have one domain or only wish to read information from your local domain. ***Note:*** When connecting to the GC, some properties (e.g. OS information) of the computers in the domain will not be copied to the database. This is because AD does not replicate them to the GC.	

9.2.2 ActiveDirectoryAttributes Section:

This section allows user defined AD attributes for Computer and User objects to be mapped onto Attribute1-10 columns of the Staging and Working ***Computers*** and ***KnownUsers*** tables.

The syntax is:

```
<ActiveDirectoryAttributes>
    <ADobjectAttributes>
        <ADobjectAttribute ADobject="Computer" ADattribute="" SQLcolumn="Attribute1" />
        <ADobjectAttribute ADobject="Computer" ADattribute="" SQLcolumn="Attribute2" />
        ....
        <ADobjectAttribute ADobject="User" ADattribute="" SQLcolumn="Attribute9" />
        <ADobjectAttribute ADobject="User" ADattribute="" SQLcolumn="Attribute10" />
    </ADobjectAttributes>
</ActiveDirectoryAttributes>
```

ADobjectAttribute element		
Name	**Description**	**Valid values**
ADobject	AD object type to be read, either from the Computers or Users containers.	Computer User
ADattribute	Name of AD attribute to be read, that is a member of the specificed AD object (*ADobject*), e.g. “distinguishedName”. No value will be read from AD if this is an empty string.	Any AD attribute name appropriate for the specified AD object. Empty string “”.
SQLcolumn	Name of SQL column where the read AD attribute value is to be inserted as a string.	Attribute1 Attribute2 Attribute3 Attribute4 Attribute5 Attribute6 Attribute7 Attribute8 Attribute9 Attribute10

Notes:

1) The AD Service will stop if there is an issue with the “clsad2db.exe.config” configuration file.
2) The AD Service will stop if the AD attribute name cannot be found in the AD Schema – the Windows Application Event Log and BJ Trace logging should help pin-point the AD attribute name causing the issue.
3) Each SQL column (Attribute1-10) is of type nvarchar(2048).
4) Some AD attribute values don’t have a value applied, they appear as “NOT SET” in ADSI Edit (a Microsoft low level directory editing tool) – these are stored in the specified SQL column as empty strings.
5) If the AD Service “*Use Global Catalogue*” option is selected, AD attribute values that are NOT *replicated* will appear to be not set and recorded as an empty string in the specified SQL column.
6) Some AD attribute values are “multi-valued” – these are stored in the specified SQL column (Attribute1-10) as bracketed values, e.g. “[*value1*][*value2*][*value3*]…[*valueX*]”.