boldonjames
by HelpSystems

User Guide
Classifier Reporting System

May 2021

Copyright Terms and Conditions

202105260146

Table of Contents

About this product

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 described in this document:
  - Classifier Event Log Service - 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.

> **NOTE:** The Classifier Reporting Event Forwarding Guide explains how event log information can be collected from your organisation.

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 - establishes 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.
- Classifier AD Service - 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 - creates event log channels that are needed to forward events to the Consolidated Event Log server.
- Migration Wizard - 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 - 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.

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 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. Familiarize yourself with the system requirements and Classifier Reporting Services installation process.
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. See the Classifier Reporting Event Forwarding Guide.
6. Create the Classifier Reporting Database with the installed Database Management component. See *The Classifier Reporting Database* on page 10.
7. Configure the Event Log Service. See *Configuring the Event Log Service* on page 16.
8. Configure the AD Service. See *Configuring the AD Service* on page 19.
9. Install Classifier Reporting Console. See the Classifier Reporting Console Guide.

Installation and System Requirements

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. See the Classifier Reporting Event Forwarding Guide. 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.

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 the Classifier Administration Guide for more details.

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

> **NOTE:** The Classifier Reporting System does not support retrieving Classifier configuration information from web locations.

Installing Classifier Reporting Services

Before You Start

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. Ensure Microsoft .NET Framework 4.7.1 or later is installed.
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, see *Upgrading the Classifier Reporting Database* on page 12 before you uninstall the earlier version.
5. If you are upgrading from version 1.0 to version 1.2, 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. See the Classifier Reporting Event Forwarding Guide for more information.

Uninstalling a previous version

1. Stop the Event Log service or the AD service if you have installed them.
2. Navigate to 'Control Panel' > 'Programs and Features'.
3. Right-click Boldon James Classifier Reporting Services and click 'Uninstall'. Confirm this operation when prompted and the product will be removed.

This will not remove the Classifier Reporting Database. See *Database Features* on page 23 for details. Do not remove the Classifier Reporting Database if you want to upgrade to a later version of Classifier Reporting Services.

If during the uninstallation, a warning is displayed stating that a set of applications should be closed before continuing, select the 'Do not close application' option and click OK.

Upgrading

If you are upgrading from an earlier version of the Classifier Reporting Services, remove the earlier version.

1. Open the Classifier Reporting Services folder in the Classifier Reporting Services bundle and run Classifier Reporting Service.exe.
2. Select which components you wish to install.
3. 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.

   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, consider entering no account details and configure the services after installation.

If the account details are not filled in, the services being installed will be configured to run as the Local System account.
The services logon do not have to be configured during installation.

4. Enter the SQL connection details.

   The services SQL authentication and connection details do not have to be configured during installation - see *Configuring the Event Log Service* on page 16 and *Configuring the AD Service* on page 19 for more details.

   The selected components will then be installed.

   If you install one or more components, a Classifier Reporting Services menu item will be created under Programs and Features.

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. In particular to licence this product, you will need a separate 'Classifier Reporting Service' licence.

See the Classifier Administration Guide on how to licence Classifier products. If you are installing the Event Log Service for the first time, follow these instructions to licence the product.

> **NOTE:** If you are upgrading fromV1.3.1 or earlier, you must relicence the Event Log Service by using the Classifier Administration tool with a new Classifier Reporting Service (CRS) licence. You cannot relicence the Event Log Service with the Classifier Reporting Tool (CRP) licence that was used for V1.3.1 or earlier of the Event Log Service.

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, see *Upgrading the Classifier Reporting Database* on page 12.

Creating the Classifier Reporting Database

The SQL Server Database must be created 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.

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:

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. 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
3. Run PrepareDatabase by running the file

   C:\Program Files (x86)\Boldon James\Classifier Reporting Services\PrepareDatabase
4. Enter the name of the server running the Classifier Reporting database. This should be localhost, if you are running the program from the server that hosts the SQL Server.
5. If your SQL Server is not listening on the default TCP port for SQL Server, enter the port that the SQL Server is listening on, to the server name. Enter Server Name and 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.
6. 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.
7. 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.
8. Press Create Database. This runs a set of SQL scripts that creates the Classifier Reporting Database.

9. When the process is finished, you should test whether the Classifier Reporting Database has been successfully created by pressing Test.
10. 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

Communicating 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.

Creating the Classifier Reporting Database by running SQL Script files

To create the Classifier Reporting Database by running SQL scripts:

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. Click OK to create the database.
4. When the database has been created, select File->Open 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.
6. After opening the scripts, click 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 *Automatic Event Processing and Deletion* on page 24) but the warnings can be ignored.

Upgrading the Classifier Reporting Database

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, 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 Services. 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. Click Test.

   The following message will be displayed if the Classifier Reporting database needs updating: "The ClassifierEventDB database is not the latest version".
8. Close the Prepare Database program.
9. If the Test button identifies that the database version is not the latest version, then click Prepare Database.
10. 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.
11. Run the migration wizard to parse the classification values in your existing Working table entries. See *Migration Wizard* on page 13.
12. Start the new Event Log and Active Directory (if using) Services
13. Install and configure the latest version of the Classifier Reporting Console onto the relevant endpoints

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.

1. Verify that the database has been backed up and that the Boldon James Event Log service is not running, then check the Verified checkbox.
2. Configure the SQL connection to the server by pressing the … button which displays the SQL Connection Editor dialog.
3. Enter the name of the server that hosts the database: If you run the migration wizard on the server that hosts the database, enter “localhost”. If you have created the Classifier Events database in an instance other than the default instance, add the name of the instance to the string, for example “localhost\instance#1”. The Database must always be ClassifierEventsDB.
4. Select either Windows or SQL Server Authentication. The windows account or SQL Server account must be configured in the database with the ClassifierSupplierRole, (see *Migration Wizard* on page 13 for details on how to configure an account with the ClassifierSupplierRole).
5. Click Test to ensure you have a connection, the click OK.
6. Click Start to start parsing label. Progress on the label parsing is displayed. Note, that 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 Close button to close the migration wizard.

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. You can 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. Click Test.

   The following message will be displayed if the Classifier Reporting database needs updating: “The ClassifierEventDB database is not the latest version”.
4. Close the Prepare Database program.
5. 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.

6. 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.
7. When the process is finished, you should test whether the Classifier Reporting Database has been successfully created by pressing the Test button
8. Restart the SQL Server Agent.

   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.

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 V1.4.0 database, you can upgrade to a V1.4.1 database.

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. Click Test.

   The following message will be displayed if the Classifier Reporting database needs updating: “The ClassifierEventDB database is not the latest version”.
4. Close the Prepare Database program.

5. Click Update Database. 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 upgraded by pressing the Test button
7. Restart the SQL Server Agent.

   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.

Updating from a Version 1.4.0/1.4.1/2.0.0 database to a Version V2.1.0 database

If you have a version V1.4.0, V1.4.1, or V2.0.0 database, you can upgrade to a V2.1.0 database.

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. Click Test.

   The following message will be displayed if the Classifier Reporting database needs updating: “The ClassifierEventDB database is not the latest version”.
4. Close the Prepare Database program.
5. Click Update Database. 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 upgraded by pressing the Test button
7. Restart the SQL Server Agent.

   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 1.4.0, V1.4.1, or V2.0.0 database to version 2.1.0.

Configuring the Classifier Reporting Services

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.

Configuring the Classifier Policy

The Event Log Service needs access to a Classifier policy for licensing and label parsing. For more information, see *Classifier Configuration* on page 7.

Configuring a Database login

You must configure the Event Log Service 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.

If you want to use Windows authentication, 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.

1. 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.
2. Grant permissions to the login to write event data to the database by mapping the account to the ClassifierSupplierRole.

Configuring the Event Log Service using the Configuration Wizard

Once you have created a database login, configure the Event Log Service using the Configuration Wizard. 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. From V1.4 and later, these values are only stored in the configuration file and are managed using the Configuration Wizard.

To configure the Event Log:

1. Open the Classifier Reporting Services Configuration Wizard, and click the Event Service tab.
2. In the SQL Connection Details area, accept the default, or click **Configure SQL Database** and either:
    - Select the Use the following SQL connection string checkbox and enter a connection string. See *Defining your own SQL Connection string* on page 18.
    - Do the following:
        a. Enter a SQL server name - 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 your SQL Server is not listening on the default TCP port, 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.
        b. Select a server logon type:
            - 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 *Configuring the Event Log Service* on page 16 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 ClassifierSupplierRole. See *Configuring a Database login* on page 16.
        c. Enter a database name - the name of Classifier Events database and should always be ClassifierEventsDB.
        d. Click Test to ensure you can connect to your database with the provided details.
3. In the Settings area:
    - Enter the Event Log Name which should be "Classifier". Alternatively, if you use the Windows Logs/Forwarded Events event channel, the value should be set to “ForwardedEvents”. Ensure the value contains no spaces.
    - Enter the Polling Interval, or the number of seconds the service waits to poll the Event Log for new events (default: 10 seconds).
    - Select the Use Bookmarking checkbox is you want to configure the service to remember the last event it processed. 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. Clearning 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.

> **NOTE:** For information on maximum number of database write retries and delay between database write retries. see *Database Connection Management* on page 19.

4. Click OK.

Defining your own SQL Connection string

If the Use the following SQL Connection String option is selected, you can 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.

See https://www.connectionstrings.com/sql-server/ provides a reference for SQL Connection strings and 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 for a list of SQL Server Connection string keywords.

> **NOTE:** If you change the SQL Connection string, retain the Initial Catalog=ClassifierEventsDB component.

Starting the Event Log Service

The Event Log service is started from the Services console.

1. 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.
2. If you want to use Windows authentication to access the database, the domain account should be associated with the ClassifierSupplierRole. See *Configuring a Database login* on page 16.

3. If you want to use SQL Server authentication, configure a Windows domain account to run the service and use the Configuration Wizard to configure the service to use a SQL Server login to access the database. See *Configuring the Event Log Service using the Configuration Wizard* on page 16. The SQL Server login must be associated with the ClassifierSupplierRole. See *Configuring a Database login* on page 16.

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

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.

Database Connection Management

Event Log Service can be 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.

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.

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.

If you want to use Windows authentication, 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.

1. 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.
2. Grant permissions to the login to write event data to the database by mapping the account to the ClassifierSupplierRole.

Configuring the AD Service using the Configuration Wizard

Once you have created a database login, configure the AD Service using the Configuration Wizard. 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. In V1.4 and later, these values are only stored in the configuration file and are managed using the Configuration Wizard.

To configure the AD Service:

1. Open the Classifier Reporting Service Configuration Wizard, and select the AD Service tab.
2. Select the Use the Event Service SQL connection details checkbox if you want the AD Service to use the same SQL connection details as configured for the Event Service. See *Configuring the Event Log Service using the Configuration Wizard* on page 16. If left unselected, leave the defaults or select Configure SQL connection and either:
    - Select the Use the following SQL connection string checkbox and enter a connection string. See *Defining your own SQL Connection string* on page 18.
    - Do the following:
        a. Enter a SQL server name - 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 your SQL Server is not listening on the default TCP port, 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.
        b. Select a server logon type:

- 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 *Configuring the Event Log Service* on page 16 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 ClassifierSupplierRole. See *Configuring a Database login* on page 19.

c. Enter a database name - the name of Classifier Events database and should always be ClassifierEventsDB.

d. Click Test to ensure you can connect to your database with the provided details.

3. Select the Use Global Catalogue checkbox if you want to configure 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.

   Do not select this option if you only have one domain or only wish to read information from your local domain. Enter the AD DC Server Name (the server that holds the Active Directory) or leave empty so the AD service will automatically locate the Domain Controller. This value is ignored if Global Catalogue is used.
4. Enter a Polling Interval value to indicate a length of time in minutes that the service waits before checking for changes in the Users and Computers AD containers (default 1 minute).

> **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.

Starting the AD Service

The AD service is started from the Services console.

1. 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.
2. If you want to use Windows authentication to access the database, the domain account should be associated with the ClassifierSupplierRole. See *Configuring a Database login* on page 19.
3. If you want to use SQL Server authentication, 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. See *Configuring the AD Service using the Configuration Wizard* on page 20. The SQL Server login must be associated with the ClassifierSupplierRole. See *Configuring a Database login* on page 19.

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

Forcing an 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.

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.

Up to 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 Database Features for details.

Database Features

Security Considerations

Database Roles

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

Role	Description
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 *Configuring the Event Log Service* on page 16 and *Configuring the AD Service* on page 19 for more details.
ClassifierConsumerRole	Logins mapped to the ClassifierConsumerRole are granted SELECT permission on the view schemas and EXECUTE permission on the stored procedures that populate the dashboards and reports. The role is intended to be used by Users that run the console. Further information can be found in the Classifier Reporting Console Guide.
ClassifierMaskedConsumerRole	Logins mapped to the ClassifierMaskedConsumerRole are granted SELECT permission on the view schemas and EXECUTE permission on the stored procedures that populate the dashboards and reports, but do not have access to masked columns. The role is intended to be used by Users that run the console 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.

Role	Description
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.

Changing ClassifierAdmin password

When the Classifier Reporting Database is created, a password is assigned to the ClassifierAdmin Logon by the installation program. We recommend that this password be changed by the SQL System Administrator.

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/

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 you can change the schedule and run the SQL job more or less frequently.

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 you can change the schedule and run the SQL job more or less frequently.

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 in the Job Properties dialog.

Indices

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.

Index creation and reorganizing

The Index creation and reorganizing job is scheduled to run once every 24 hours. When the job runs, the following happens:

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, nothing occurs. If you want to re-create the indices or if you want to add your own indices to the procedure, 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.

2. Runs the usp_ReorganizeIndices stored procedure to defragment the indices.

This will defragment the indices. It is possible to change how frequently the job is run. For example if you think that the indices 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 indices, disable and/or remove the job after creating the database.

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. 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.

Other Considerations

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 *Other Considerations* on page 27.

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 of a live system with a database of approximately 7 million events, the average storage required for each event is approximately 2,263 bytes per event and this is likely to decrease as the number of events in the database increases.

Calculating the amount of disk space required

Consider the following

Number of Users	= NU
Number of Events per day	= Nd
Number of Week	= Nw

The number of events created in such an organisation is

Ne = Nu * Nd * 5 * Nw

For example, consider an organisation with 2000 Users that generated, on average 50 events per day each. The total number of events for a six-month period would be

Ne = 2000 * 50 * 5 * 26 = 13,000,000 events.

Assume every event uses 2,263 bytes, 13,000,000 events would require 2263 * 13,000,000 = 29,419,000,000 bytes of disk space, which is approximately 27.4 Gb. This may be an overestimate because the average the storage requirement per event decreases if more events are stored in the database.

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.

Other SQL Scripts

The Classifier Reporting Services includes 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.

SQL Script	Description
NumberOfRows.sql	shows the number of entries in all tables of the Classifier Events Database.
DeleteAll.sql	deletes 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	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	contains a set of procedures that can remove duplicate event from the database. See *Removing duplicate copies of events* on page 28 for more details.

Removing duplicate copies of events

The Classifier Events Database can erroneously contain multiple copies of the same event. 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 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.

Script	Description
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.

NOTE: Events that look identical are actually distinct events that differ by an extremely small time margin.

If you do observe multiple copies of the same events, we recommend that you review your event collection system and use these procedures as a last resort.

Removing the Classifier Events Database

To remove the Classifier Events Database from your SQL Server:

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. Running SQL Server Management Studio, and from the left-hand pane, select SQL Server Agent->Jobs to remove all the SQL jobs (see *Other Considerations* on page 27).
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

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.

Appendix - Configuration Wizard – Classifier configuration settings

The Configuration Wizard allows the Classifier configuration settings that are stored in the registry at:

HKLM\SOFTWARE\Wow6432Node\Boldon James\ConfigManager\ServiceMode to be easily changed.

To change the configuration settings:

1. Open the Classifier Reporting Services Configuration Wizard, and select the Classifier tab.
2. Select the Enable advanced settings editing (Expert Mode) check box.

   > **NOTE:** This checkbox is disabled by default to prevent accidental changes.

3. Configure the following:
   - ServerRootType - a 32bit unsigned integer (REG_DWORD) describing where the Classifier Configuration is obtained from. Valid values are:
     File System – Classifier Configuration is stored on local filesystem.
     Active Directory – Classifier Configuration is stored in Active Directory.
   - Configure the following:
   - ServerFileSystemRoot - a string (REG_SZ) that contains the filesystem path pointing to the directory containing the Classifier Configuration folders and files – this is only used when ServerRootType=0.
   - LabelConfiguration - a string (REG_SZ) that contains the name of the Classifier Label Configuration to be used.
   - Policy a string (REG_SZ) that contains the name of the Classifier Policy to be used.
4. Click Write registry settings to save the configuration data to the registry. This cannot be undone. The Enable advanced settings editing checkbox is reset to the default; that is, no changes are saved. Clearing this checkbox this will lose any unsaved changes.

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**

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services\clsev2db.exe.config		
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.	50
PollingInterval	Number of seconds the service waits to poll the Event Log for new events.	10

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services\clsev2db.exe.config	
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"

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services\clsev2db.exe.config		
	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.	

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:

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

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services\clsad2db.exe.config	
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).

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services\clsad2db.exe.config	
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>;" />

File: C:\Program Files (x86)\Boldon James\Classifier Reporting Services\clsad2db.exe.config	
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.

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

ADobjectAttribute element		
ADattribute	Name of AD attribute to be read, that is a member of the specified 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

NOTE:

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]”.