Boldon James
A QINETIQ company

Classifier Evaluation Guide

UM645200

May 2019

© Boldon James Ltd. All rights reserved.

Customer Documentation

This document is for informational purposes only, and Boldon James cannot guarantee the precision of any information supplied.
BOLDON JAMES MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Contents

1 Introduction 4
1.1 OWA and Notes Classifier 5
1.2 Classifier Document References 5
2 Stage 1 - Establish an initial system 6
2.1 Configure the Test System Environment 6
2.1.1 Office 2010 / Windows 2008 R2 / Window 7 7
2.2 Configure your Active Directory Environment 7
2.3 Install Classifier Administration Server 8
3 Define a Classifier Configuration 9
3.1 The Classifier Administration Web interface 9
3.1.1 Operation of the Classifier Administration interface 9
3.2 Creating a new Classifier Configuration 10
3.3 Creating the Selectors for Labels 13
3.3.1 Creating the Classification selector 13
3.3.2 Creating the Department Selector and values 16
3.4 Defining Marking Formats 16
3.4.1 Configure the Summary Marking Format 17
3.4.2 Configure the Standard Marking Format 19
3.5 Defining a Policy to deploy to users 21
3.5.1 Defining which Selectors are available in the policy 23
3.5.2 Defining Marking Rules 25
3.5.2.1 Word Header Rule 26
3.5.2.2 Word Footer Rule 29
3.5.2.3 Email FLOT rule 29
3.6 Application and Global Settings 30
3.7 Locally testing the policy 32
3.8 Deploying the Configuration 35
3.8.1 How the configuration reaches the client environment 36
3.9 Publish Configuration 37
3.9.1 Publish Configuration to File Store 37
3.9.2 Set the permissions to allow clients to read the configuration 37
4 Client Environment Configuration 39
4.1 Registry Key locations and precedence 39
4.2 Setting the Registry Keys for this test environment 40
4.2.1 Set the Registry keys directly 40
4.2.2 Set the Registry keys using Group Policy 41
4.2.2.1 Client Registry Settings 45
5 Verify Initial Client Functionality 46
5.1 Configure Client PC 46

5.2 Install Classifier 46

5.3 Confirm the installation of Classifier on the client PC 46

6 Demonstrate Functionality Changes. 47

6.1.1 Configure User Message 47

6.1.2 Define Rule to Perform label validity checks for emails 48

6.1.3 Disable Show the label dialog when mandatory label 52

6.1.4 Demonstrate the additional features 53

7 Email Domain Clearances 56

7.1 Ensuring Clearance Check Email Domains is enabled 56

7.2 Configure an Email Domain Clearance 56

7.3 Establish Rule to perform recipient clearance checks when sending email 58

7.3.1 Establish a Message for use in the Rule 58

7.3.2 Establish Recipient Clearance Check Rule 59

7.3.3 Locally test the changes 60

7.4 Publish the configuration and test the client environment 61

8 Active Directory Changes 62

8.1 Extend the Active Directory Schema 62

9 Deploy Configuration via Active Directory 63

9.1 Publish Configuration to Active Directory 63

9.2 Change Registry Settings for Configuration Location 64

9.2.1 Change Registry Directly 64

9.2.2 Setting Registry using Group Policy 64

9.2.2.1 Changed Client Registry Settings 67

1 INTRODUCTION

Administrators should read this document to gain an understanding of how to configure and deploy Classifier applications. It assumes the reader is familiar with the terminology introduced in the Suite Overview, reference [3].

This document describes the Classifier Administration Server component that provides manipulation of the Classifier Configuration via a web interface.

To get the most out of this guide, use a dedicated test environment including client desktops.

This evaluation guide describes how to create and configure an environment (CLASSIFIER.TEST AD domain) with a Classifier Configuration (Classifier Test) and a single deployment policy (All users). If you configure your system as described, you will arrive at a working system that you can then use for evaluation or testing. It demonstrates features such as:

- Deployment of configuration via Active Directory
- Starting with an empty Configuration Template rather than a pre-populated Configuration Template as used in the Getting Started Guide.

Note: This Guide only makes use of Email and Office Classifier product licences.

The guide consists of three stages. Each stage yields a working solution with the subsequent stages implementing additional Classifier functionality and/or alternative administration mechanisms. The stages are as follows:

Stage 1 (Sections 2, 3, 4, 5 and 6)

- Establish system environment [Section 2]
- Classifier Configuration of Labelling features [Section 3]
- Deploy (Publish) Configuration via shared File Store [Section 3]
- Client environment Configuration [Section 4]
    a) Setting Registry keys directly

    OR

    b) Use of Group Policy to set Registry Keys
- Demonstrate client operation [Section 5]
- Demonstrate change of configuration to use additional features [Section 6]

Stage 2 (Section 7)

- Implement Domain Clearance Checking for external recipients [Section 7]
- Demonstrate client operation [Section 7]

Stage 3 (Sections 8 and 9)

This stage covers features that require Active Directory Schema update

- Extend Active Directory Schema and set permissions [Section 8]
- Deploy (Publish) Configuration via Active Directory. [Section 9]

1.1 OWA and Notes Classifier

As stated above, this document describes evaluation in a Microsoft Office desktop environment. However, most of the Classifier Administration features and mechanisms used in this document are the same for OWA Classifier and Notes Classifier; this document can be used an aide to guide you through familiarisation for those products.

Exploring the effects under Lotus Notes requires installation of the Notes Classifier server component, applying a Notes Classifier licence, and enabling the **Global Settings / Application Settings / Lotus Notes** option within the Classifier configuration.

For OWA, read reference [1] in conjunction with section 4. This provides full details on OWA Classifier Administration features.

Section 5 is not relevant to OWA; the OWA test server requires access to the published configuration in order to view the changes to the end user experience.

1.2 Classifier Document References

[1] Administration Server Guide (UM6351)

[2] Planning Considerations (UM6354)

[3] Suite Overview (UM6352)

2 STAGE 1 - ESTABLISH AN INITIAL SYSTEM

This stage establishes a minimal operating Classifier system. The steps are:

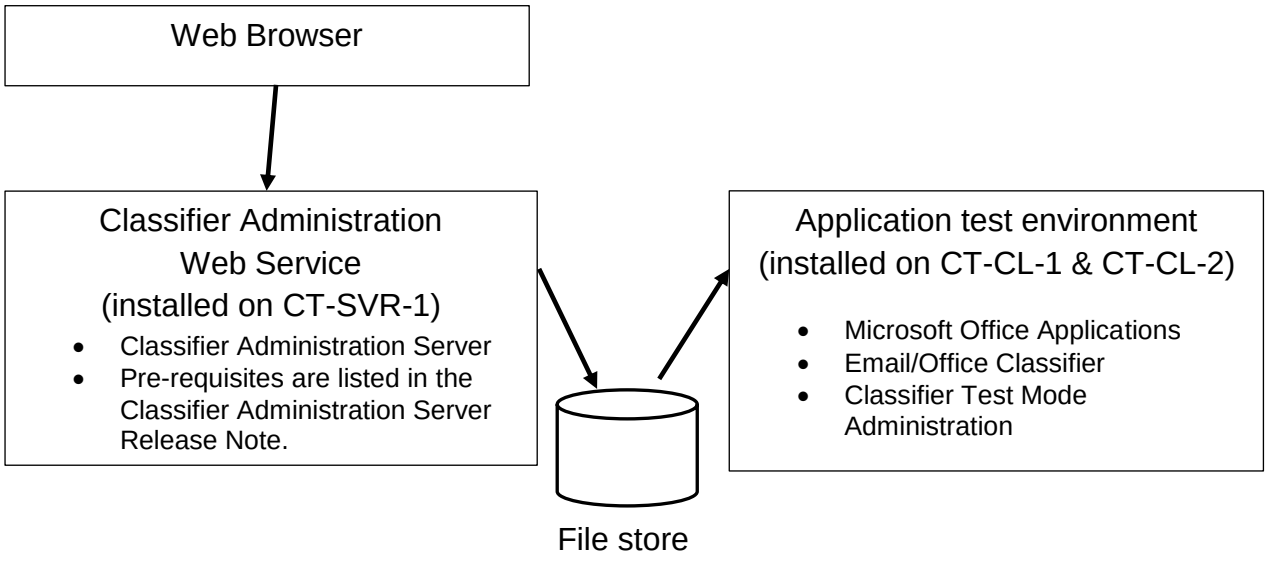
- Configure the system test environment and install Classifier Administration (Section 2)
- Define the Classifier configuration (create Selectors and Values, Marking Format, Policy, Application and Global settings) (Section 3)
- Test the policy locally (Section 3)
- Publish the configuration via file store (Section 3)
- Configure the client environment (Section 4)
- Install Office Classifier and Email Classifier (Section 5)
- Verify client functionality using the published configuration and policy (Section 5)

2.1 Configure the Test System Environment

Complete the following tasks to prepare your Classifier test environment. The computers used in this case study are in a domain called **CLASSIFIER.TEST** and assumed to have the following names:

- ❑ A domain controller – referred to as **CT-DC-1**.
- ❑ A server – referred to as **CT-SVR-1**.
- ❑ Two client PCs – referred to as **CT-CL-1** and **CT-CL-2**.

The following framework is required In order to evaluate Boldon James Classifier:



This case study is applicable to any supported environment: Windows client, Windows server, Office, .NET. You should consult the Classifier Server Administration, and Email and Office Classifier release notes for definitive information with regard to versions and Service Packs supported.

The sub-section below shows an example environment. Use the contents of the tables as a guide whilst configuring the environment, adjusting to suit your local circumstances within the platforms supported by Classifier. The tables outline the computer names, operating system, IP settings and DNS settings, and provide an overview of the baseline setup.

The evaluation process is unaffected by the environment other than where the Office application interface varies between versions. The vast majority of this document is unaffected by the environment. Documentation clearly indicates where the steps vary according to the base environment.

2.1.1 Office 2010 / Windows 2008 R2 / Window 7

Computer Name	Operating System & Software Requirements	IP Settings	Notes
CT-DC-1	Windows Server 2008 R2, Exchange 2010	IP address: 10.0.0.1 Subnet Mask: 255.255.255.0	CLASSIFIER.TEST domain controller – Active Directory.
CT-SVR-1	Windows Server 2008 R2 .NET 4.7.1	IP address: 10.0.0.2 Subnet Mask: 255.255.255.0	Member of CLASSIFIER.TEST domain.
CT-CL-1	Windows 7, Office 2010 .NET 4.7.1	IP address: 10.0.0.3 Subnet Mask: 255.255.255.0	Member of CLASSIFIER.TEST domain.
CT-CL-2	Windows 7, Office 2010 .NET 4.7.1	IP address: 10.0.0.4 Subnet Mask: 255.255.255.0	Member of CLASSIFIER.TEST domain.

2.2 Configure your Active Directory Environment

Use the following example structure as a reference to configure Organisational Units, Groups and Users on **CT-DC-1**:

dc=CLASSIFIER, dc=TEST

ou=Departments

ou=Engineering

ou=Sales

cn=Board @ security group

The tables below list the users within each organisational unit and group:

Organisational Unit	User Name
Engineering	EngineeringUser1 Engineeringuser2 EngineeringVP
Sales	SalesUser1 SalesUser2 SalesVP

Note: Each user requires a Microsoft Exchange mailbox to be set up on CT-SVR-1

Configure the following security group below the 'Departments' organisational unit and add the users to the group:

Group	User Name
Board	SalesVP EngineeringVP

Configure Outlook to operate in online (non-cached) mode.

Note: You should check that all test users and the Administrator can send and receive e-mail using both client PCs prior to installing and configuring Classifier functionality.

2.3 Install Classifier Administration Server

The Classifier Administration Server performs Classifier configuration. A web browser provides access to this through a web service. To install Classifier Administration Server:

- ❑ Logon to CT-SVR-1 as a user with suitable privileges (e.g. CLASSIFIER.TEST administrator account).
- ❑ Establish an administration user (e.g. ClassAdmin) for the Classifier configuration.

  This user will require read/write access to any file locations used for the import/publishing of Classifier Configurations – established later in this document.
- ❑ From the Classifier Base Bundle open **Classifier Server Administration** folder and run **ClassifierAdministrationServer.msi** (or Setup.exe). Follow the wizard installation steps to complete the install.
- ❑ Check that the system intended to host the Classifier Administration Server product has all the pre-requisites installed as defined in the Classifier Administration Server release notes.
- ❑ Follow the wizard installation steps to complete the install.
- ❑ Check that the Classifier Administration Service has a status of ‘Started’.

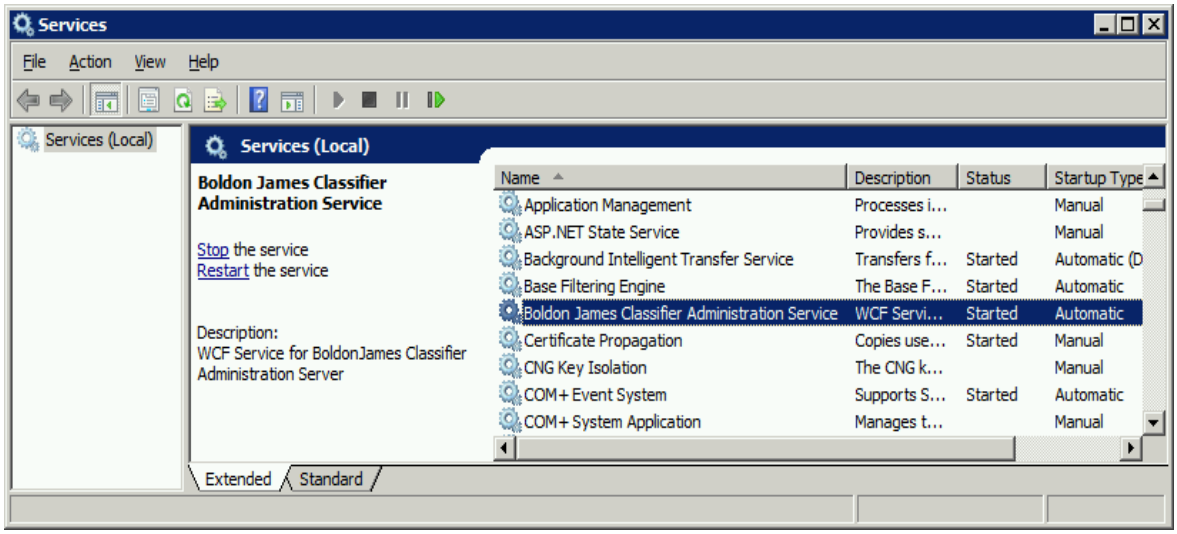


Figure 1: Services

3 DEFINE A CLASSIFIER CONFIGURATION

3.1 The Classifier Administration Web interface

A Web interface that connects to the Classifier Administration Service provides Classifier configuration.

Logon to CT-CL-1 as ClassAdmin.

From the start menu type in http://CT-SVR-1 and click **enter** to connect to the Classifier Administration Service. The following dialog appears:

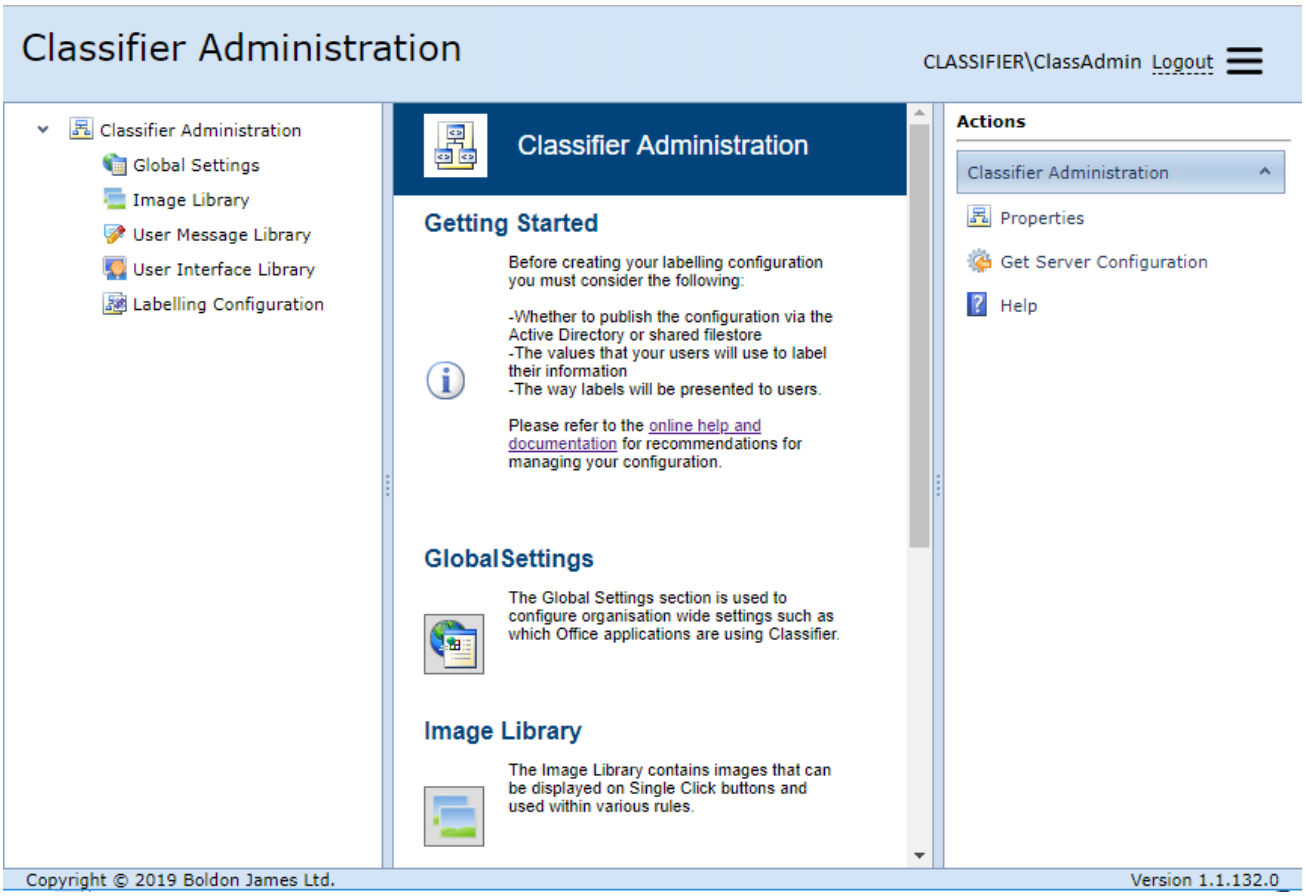


Figure 2: Initial state

3.1.1 Operation of the Classifier Administration interface

Throughout this document, the instructions will direct you to select a particular Classifier Administration action from the **Actions Pane**.

At the top of the Actions Pane a list of actions is presented relevant to the item selected in the left hand pane: for example, **User Message Library** - **Add a new message** in the figure below.

At the bottom of the Actions Pane, a list of actions is presented relevant to the item selected in the middle pane. For example, **Item** - **Properties**, **Copy** and **Delete** in the figure below.

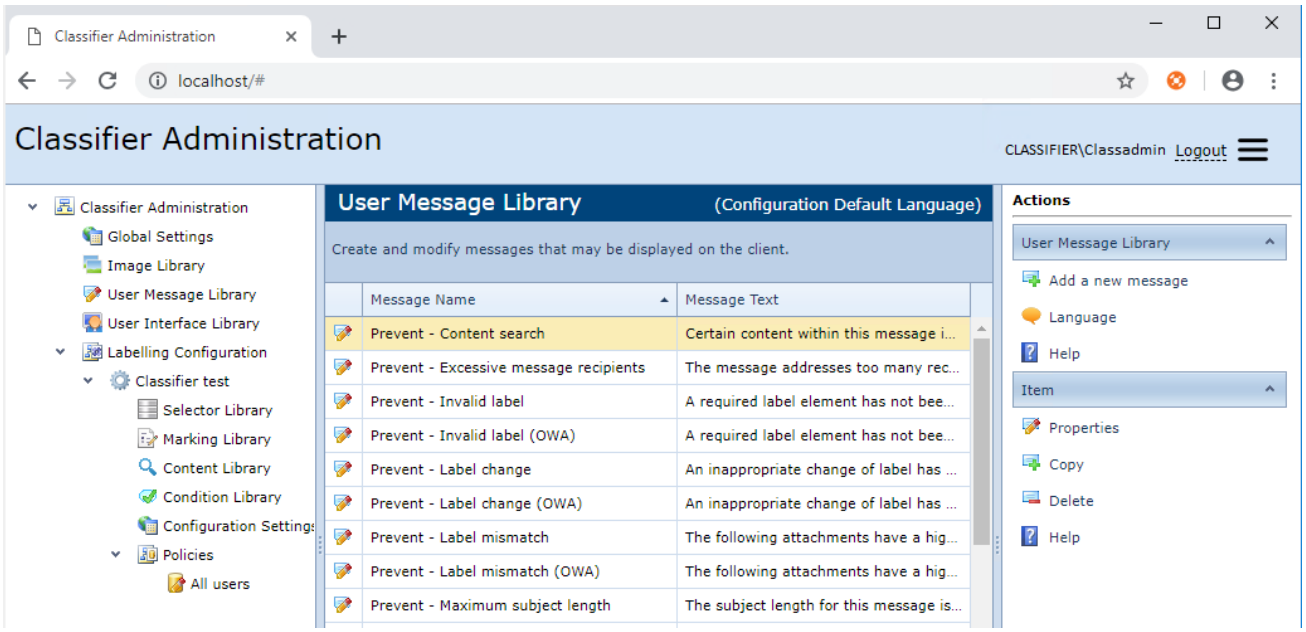


Figure 3: Action examples

3.2 Creating a new Classifier Configuration

- ❑ Starting with the empty Classifier configuration shown in Figure 2.
- ❑ Select the **Labelling Configurations** node and select **Add a new label configuration** action. This displays a dialog.
- ❑ Enter a configuration name – **Classifier test**
- ❑ Select **Category → Miscellaneous** and template **Empty Configuration**.

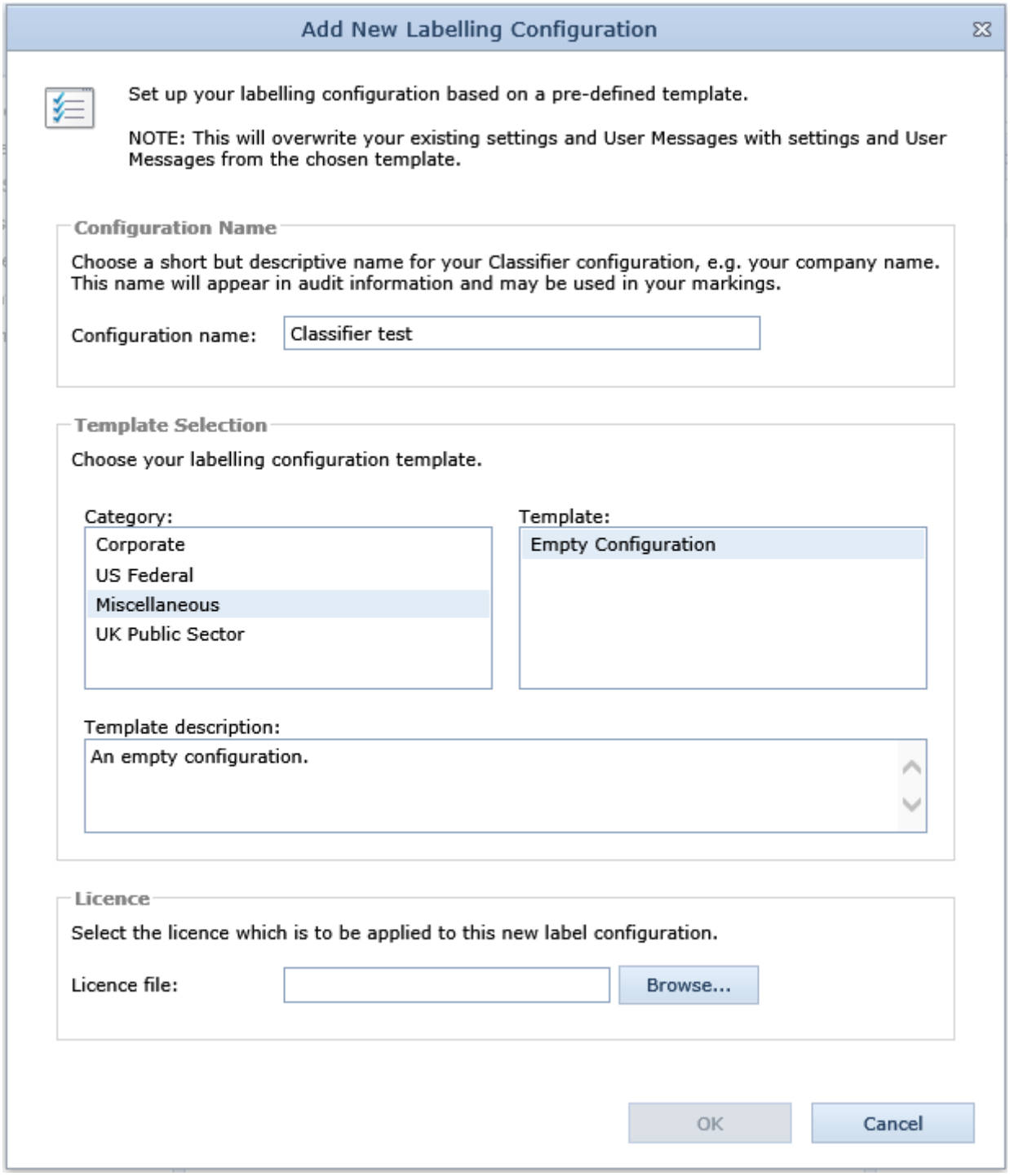


Figure 4: Template selection

- ❑ We need to apply a Classifier licence. In this instance, use the limited duration evaluation licences from the **Licence** folder in the **Base Bundle**.
- ❑ Click the **Browse** button and navigate to the **Licence** folder in the **Base Bundle**.
- ❑ Note that each licence appears in its own sub-folder below the parent **Licence** folder. **Open** the Office Classifier sub-folder and select the **IMPCOF.LIC** file.

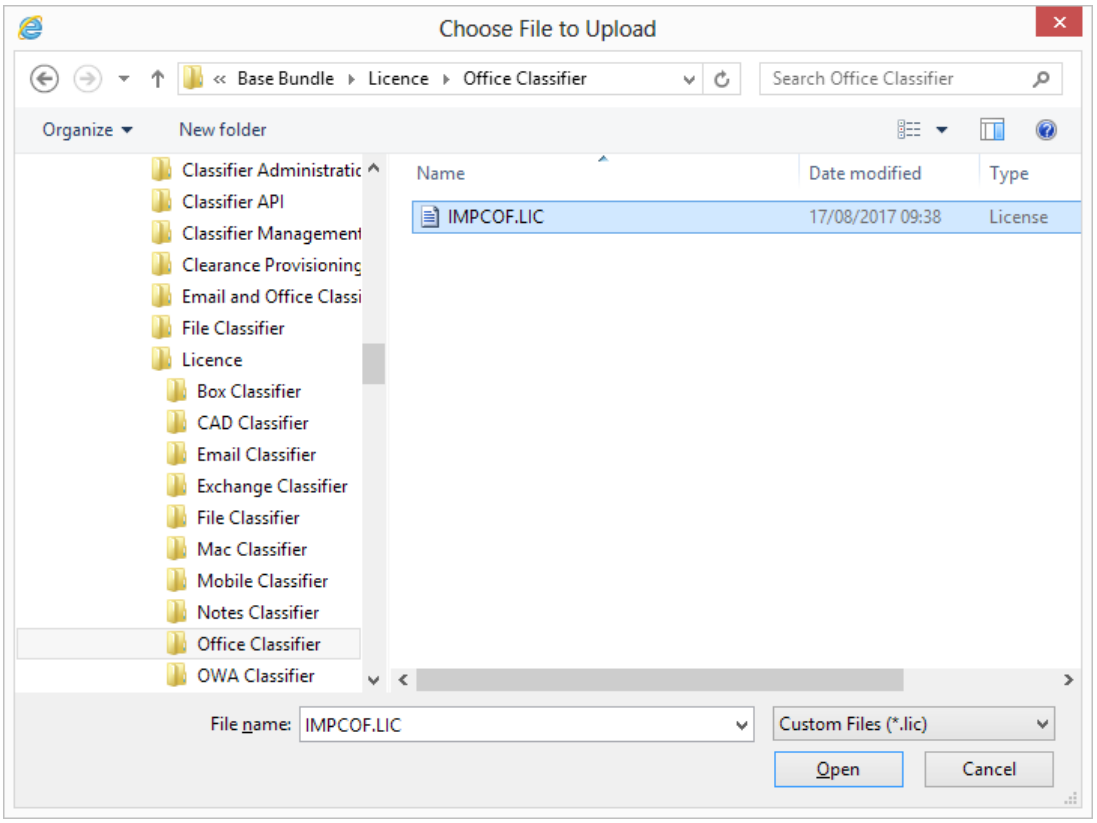


Figure 5: Licence folder dialog

- ❑ Click **OK**. The Labelling Configuration appears:

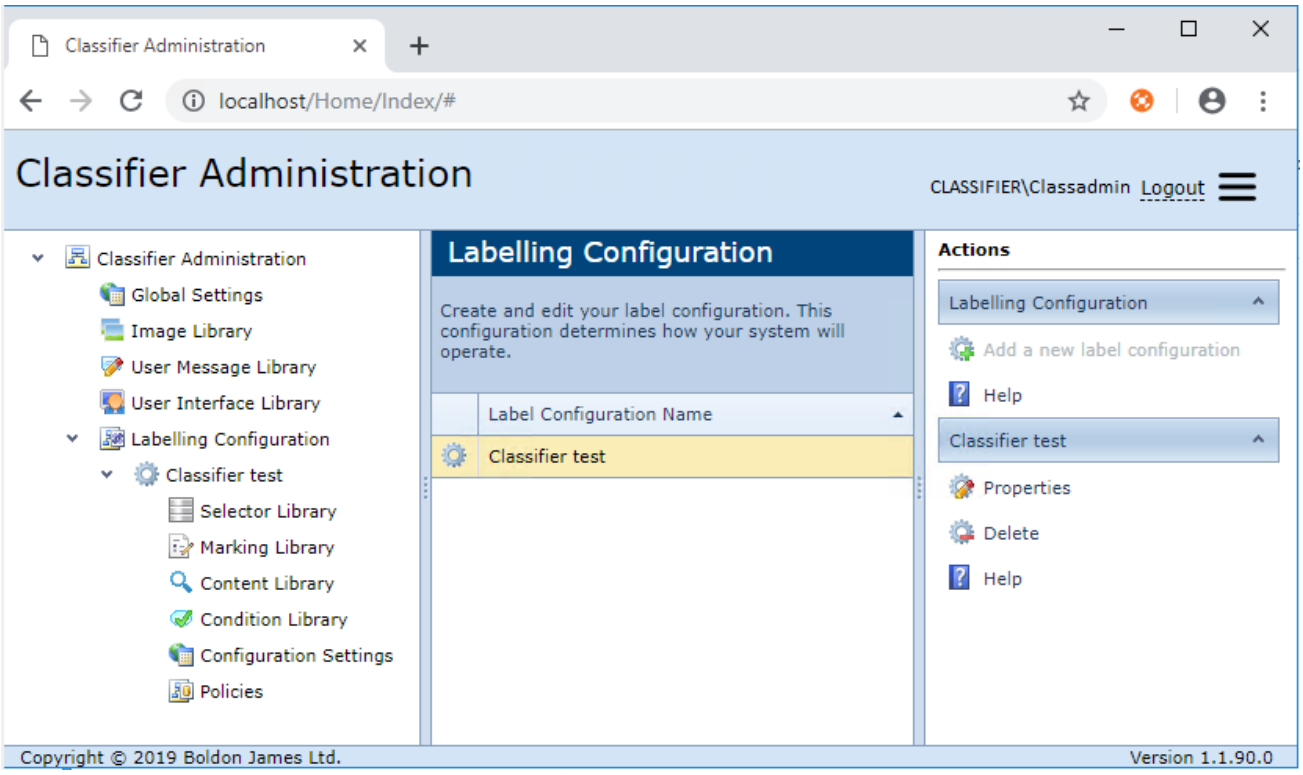


Figure 6: Classifier test Configuration

- ❑ Now add a licence for **Email Classifier**.
- ❑ Select **Global Settings**.

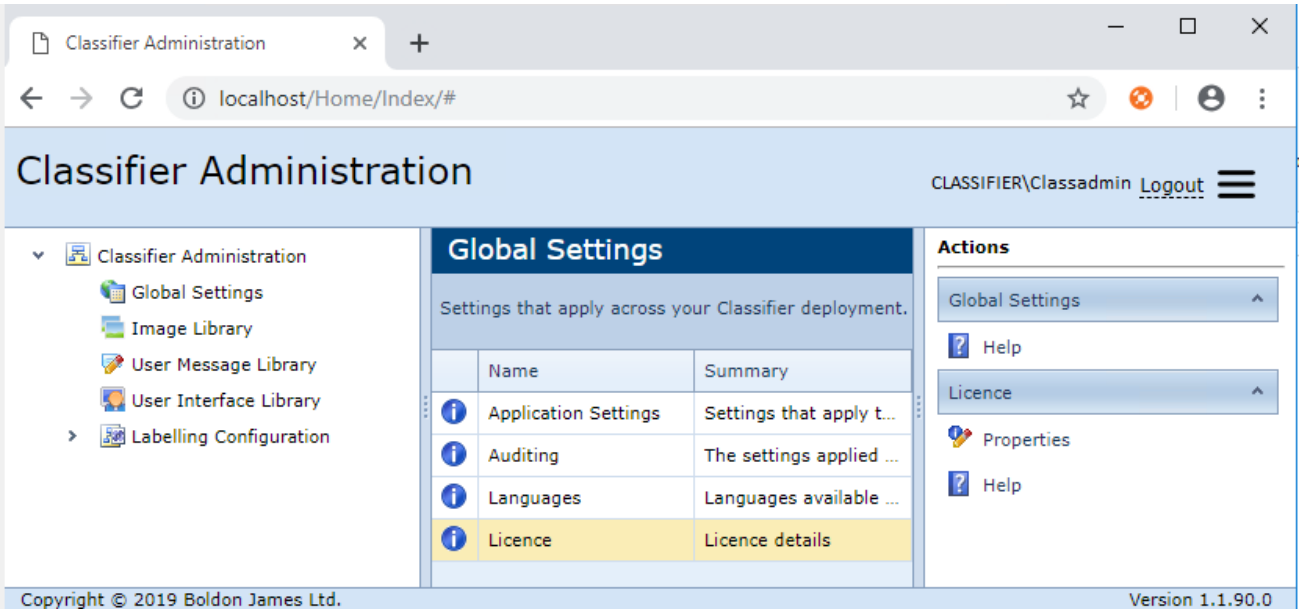


Figure 7: Apply Licences – Global Settings

- ❑ Open **Licence**. The dialog allows you to apply one or more licences.
  Click **Add/Update** and add the IMPCEM.lic file (This is the Email Classifier license).

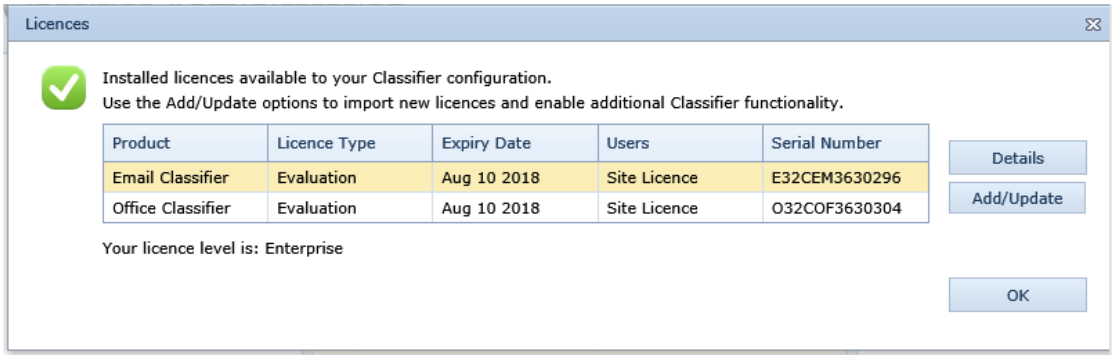


Figure 8: Apply Licences – Licences added

- ❑ Click **OK** to apply the licence changes and return to the main dialog.

3.3 Creating the Selectors for Labels

This sequence creates two Selectors called **Classification** and **Department**

3.3.1 Creating the Classification selector

- ❑ Select the **Selector Library** and choose **Add a new selector/Single selection list**.
- ❑ This presents you with the following dialog:

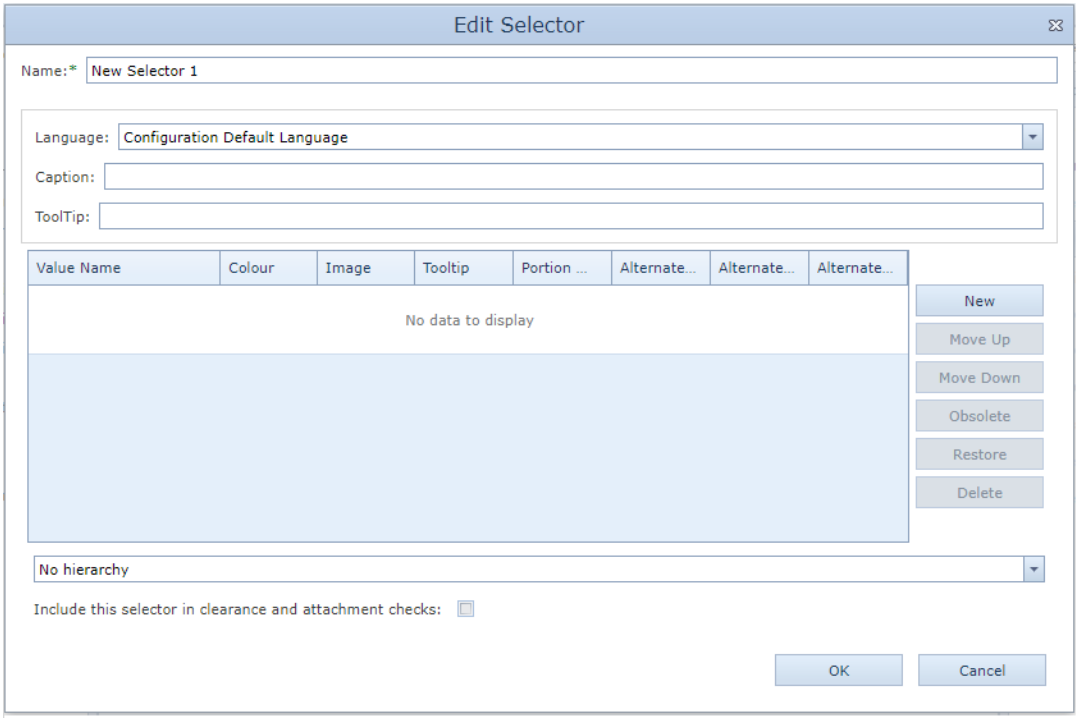


Figure 9: New single selection list

- ❑ Fill in the **Name** field as **Classification** and **ToolTip** with "**This indicates the sensitivity of the content**".
- ❑ Now add the selector values.
- ❑ Click **New**. An Edit Form is presented:

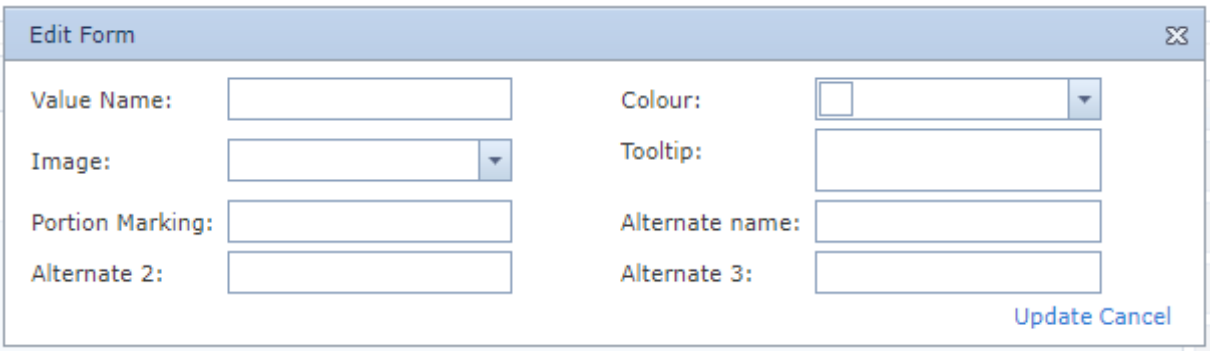


Figure 10: Edit single select selector value

- ❑ Replace **New Value 1** with **Public**.
- ❑ **Tab** to the Colour cell and set the colour to **Green** using the available drop down.
- ❑ Click **Update** and the entry in the main list is updated.
- ❑ Repeat the sequence to add two **New** selector values:

Value Name	Colour
Internal	Yellow
Confidential	Red

- ❑ The main list should then show:

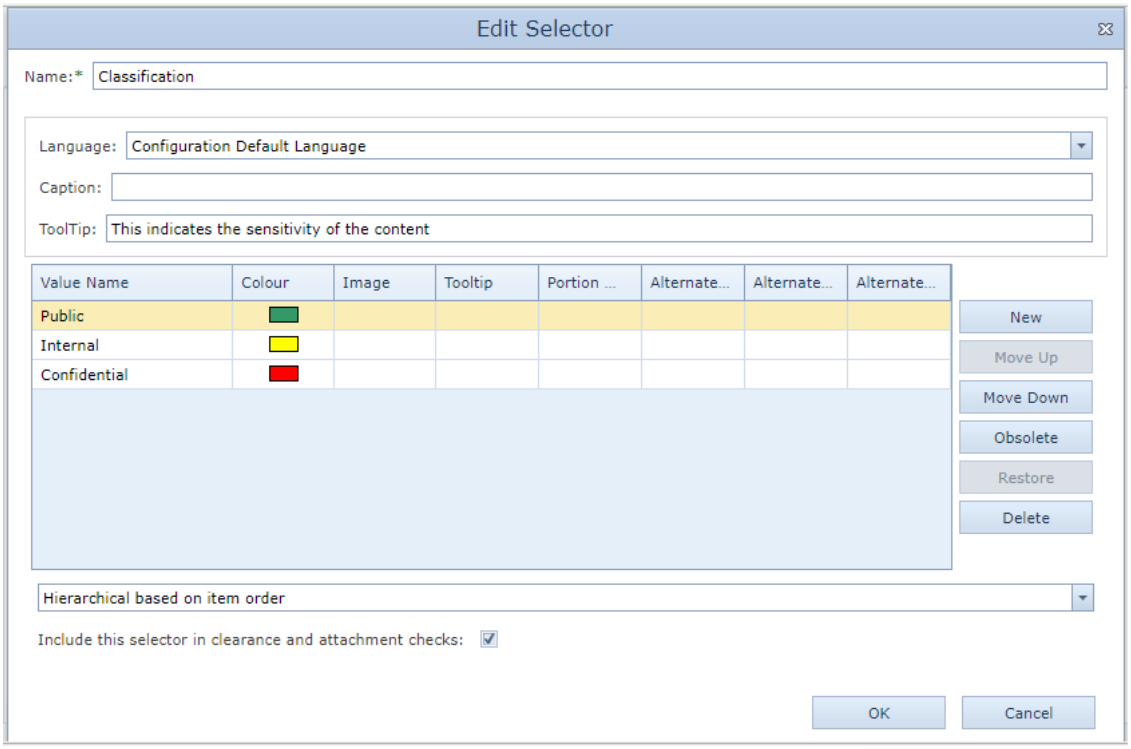


Figure 11: Classification selector values

- ❑ Select the **Hierarchical based on item order** setting in the Hierarchy drop down.
- ❑ Check **Include this selector in clearance and attachment checks** as this selector is to be included when Clearance checks are performed (sections 7, 10 and 11).
- ❑ Click **OK** – the list of items will appear in the parent screen

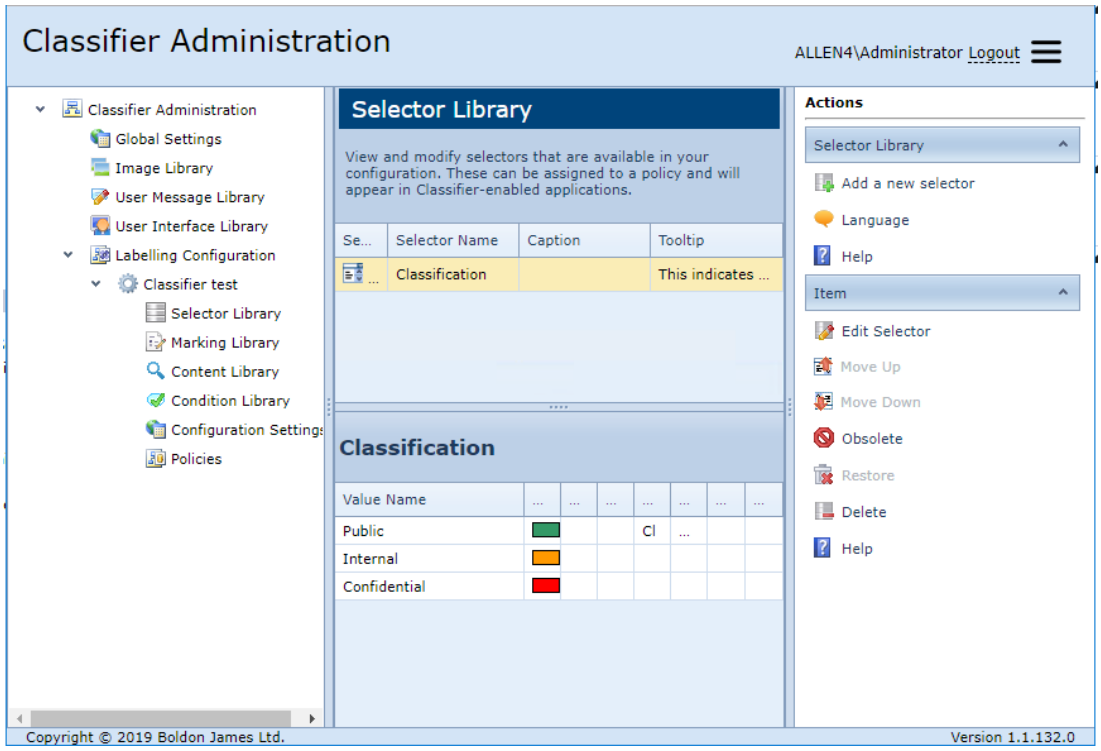


Figure 12: Classification Values List

3.3.2 Creating the Department Selector and values

- ❑ Repeat the sequence in 3.3.1 above to create a second Selector with **Name** = **Department** and **ToolTip** = "**Choose the Department that produced the content**".
- ❑ For this second Selector establish the following Department values:
  - **Sales** Leave the colour as default.
  - **Engineering** Leave the colour as default.
  - **Board** Leave the colour as default.
  - Ensure the hierarchy setting is **No hierarchy**
- ❑ Check **Include this selector in clearance and attachment checks** as this selector is to be included for Clearance checks.
- ❑ Click **OK** and the values will appear in the parent screen showing the Department selector and values

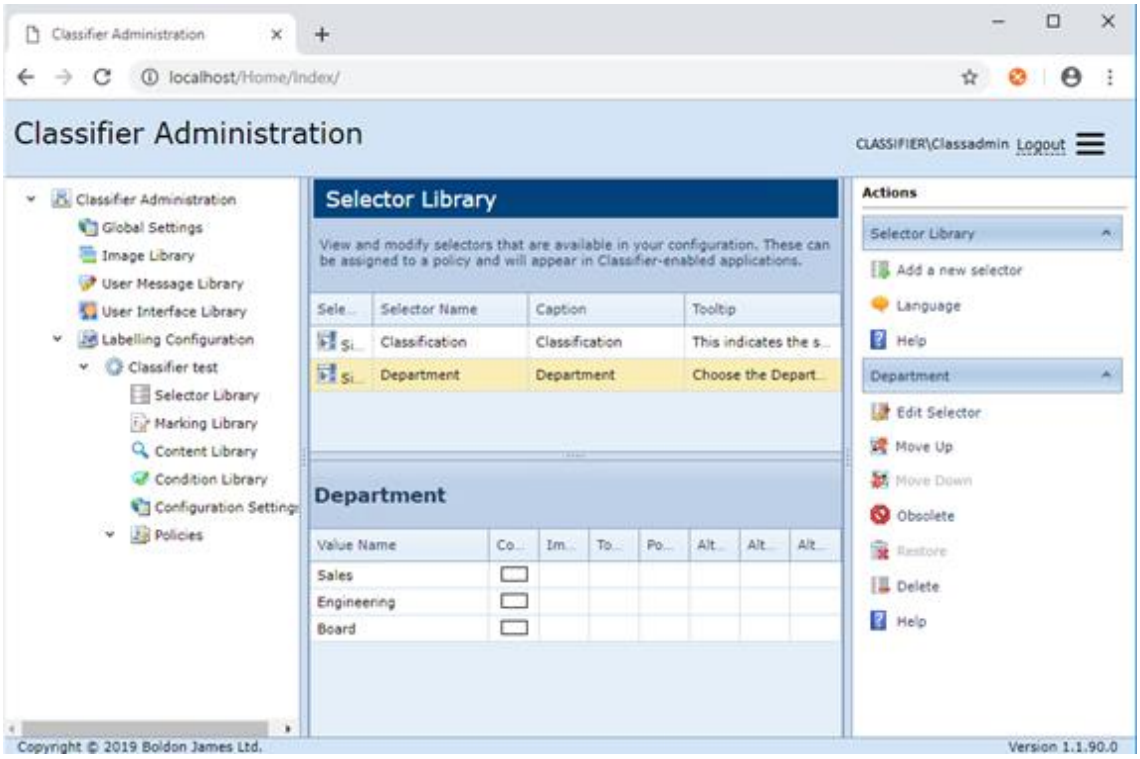


Figure 13: Department Values List

3.4 Defining Marking Formats

Use Marking Formats to configure how labels appear to users, e.g.:

a) To represent the current label value in various transient places (e.g. Outlook Information Bar).

b) To insert Headers/Footers/FLOT into documents / emails.

You can use one Marking Format across the whole configuration or different Marking Formats to give different renderings according to your requirements. For example, the Header and Footer could be different.

The **Empty Configuration** template includes a placeholder **Summary Marking** Format used when Summary Label values appear (e.g. Outlook Information Bar). The **Summary Marking** forms a

basis to configure a separate **Standard Marking** referenced by various rules (e.g. Document Headers).

3.4.1 Configure the Summary Marking Format

- ❑ Select **Marking Library** and select the **Summary Marking** entry. Click **Properties** which will present the following:

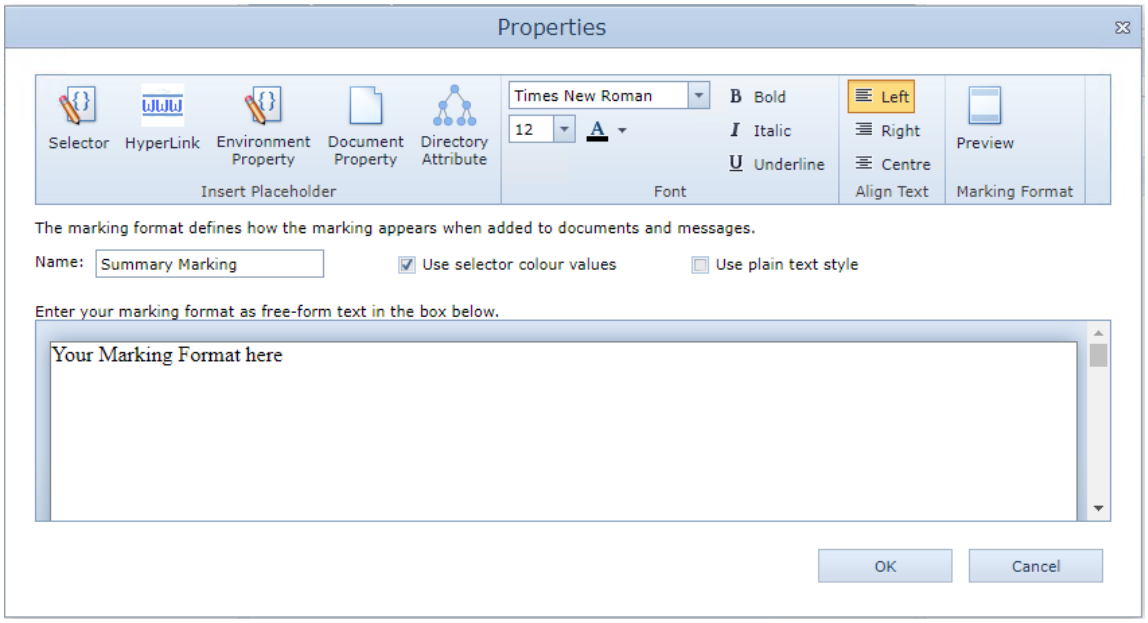


Figure 14: Summary Marking Properties

- ❑ Delete the text 'Your Marking Format here', and then click **Selector (Insert Placeholder)** which presents a list of available Elements.

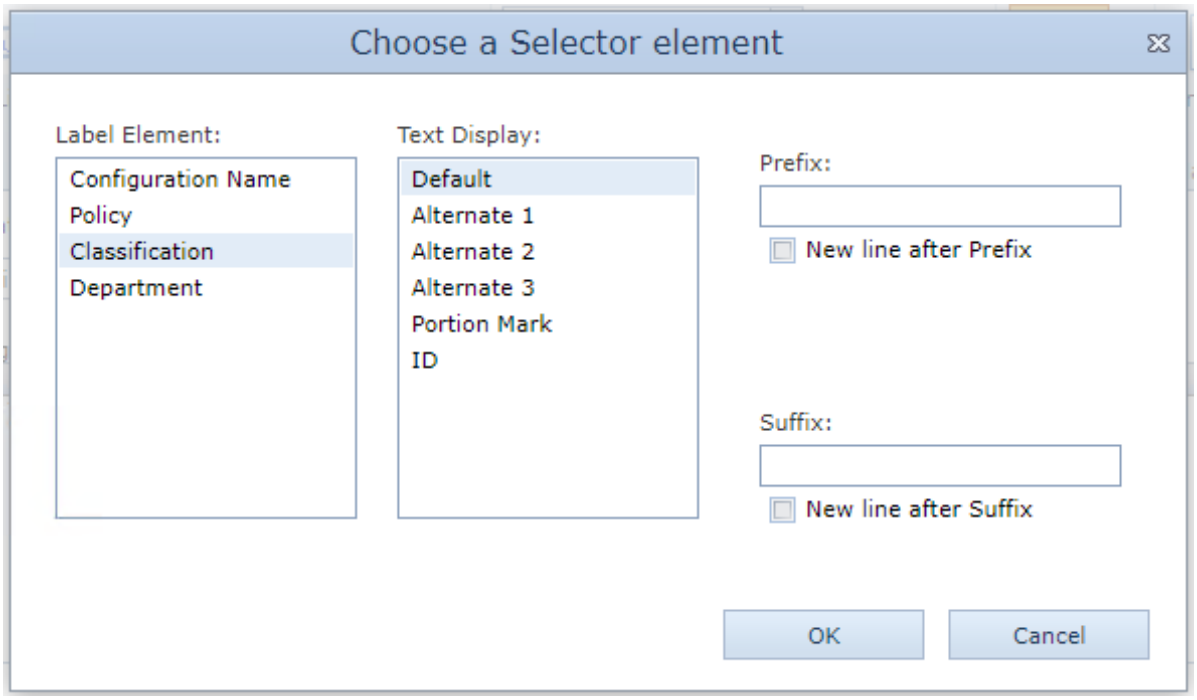


Figure 15: Choose a Selector element

- ❑ Select **Classification** and click **OK** to insert a placeholder in the marking format:

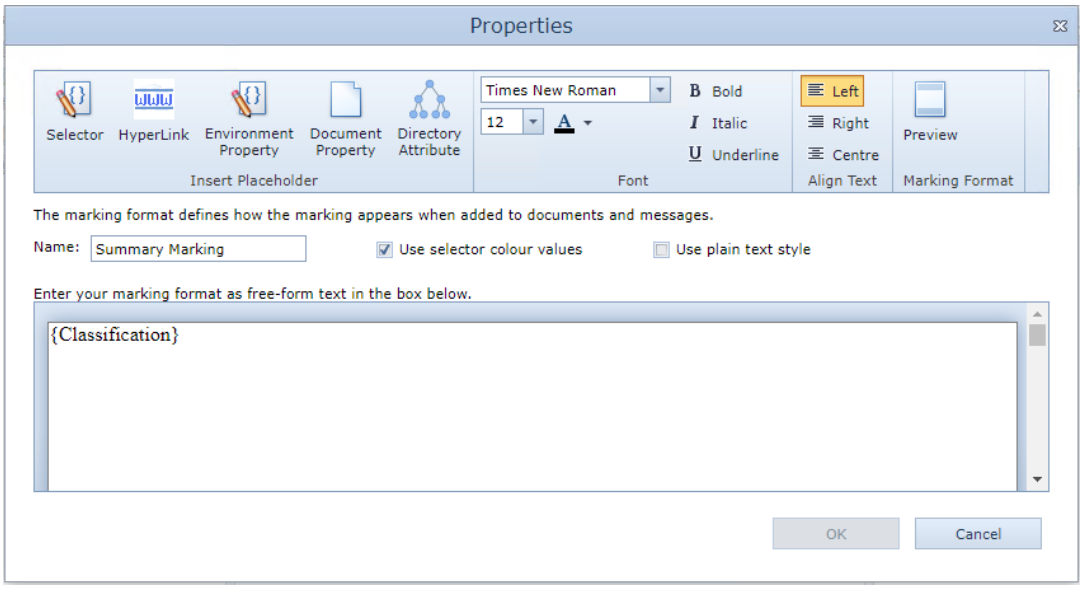


Figure 16: Classification inserted into Marking

- ❑ Enter a single "**space**" after the {Classification} placeholder.
- ❑ Repeat the **Insert Selector** process once to add the **Department** element to leave the following:

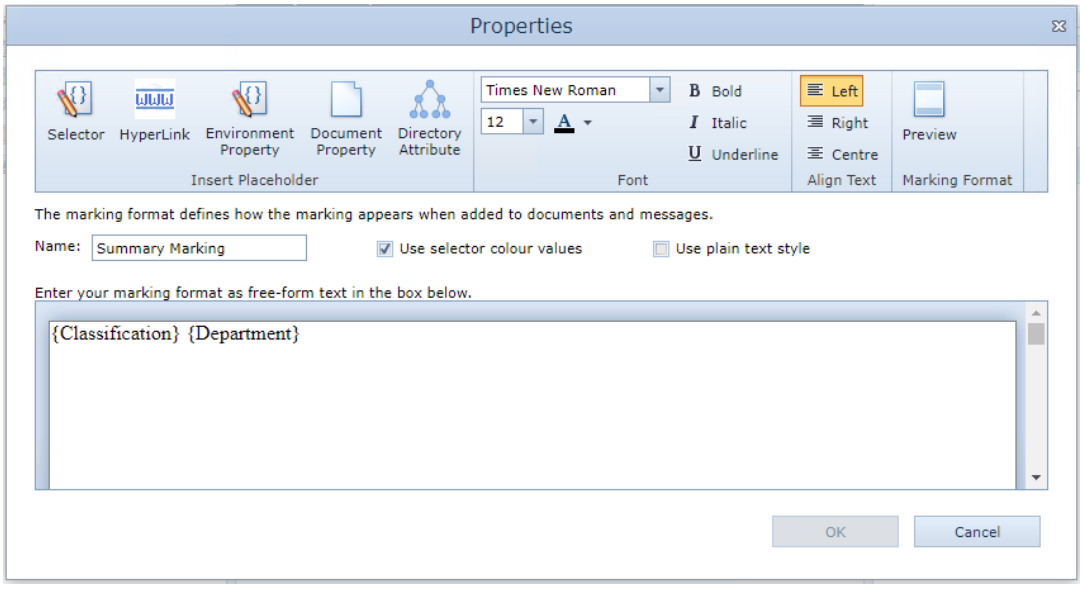


Figure 17: Summary Marking Format configured

- ❑ In this instance, we are leaving the fonts unchanged. The Selector library defines the colours of Selector values.
- ❑ You can preview the appearance of the marking format by selecting the **Preview** button.

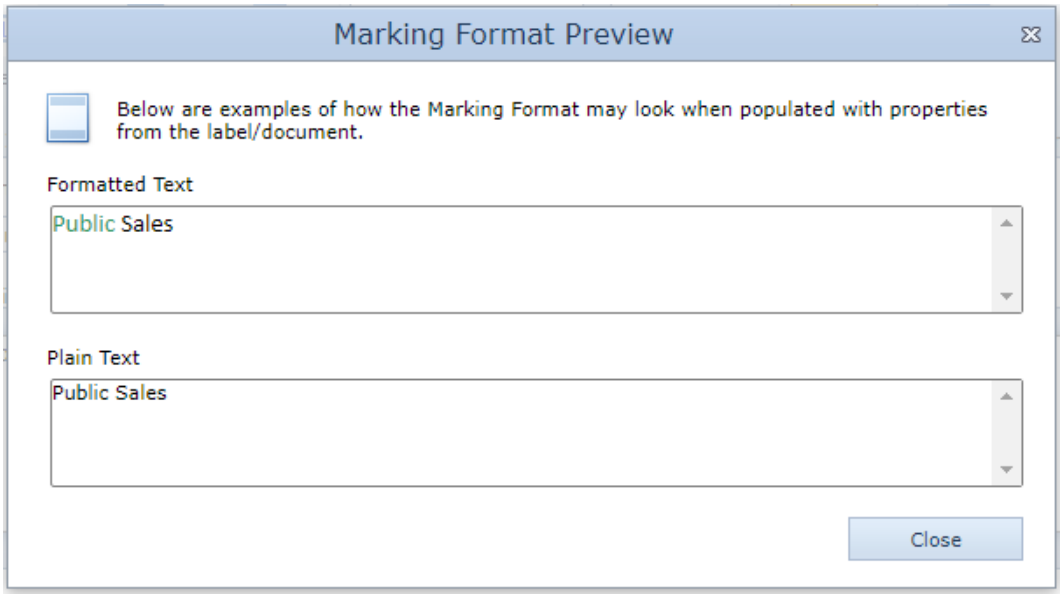


Figure 18: Marking Format Preview

- ❑ Click **Close** for the Marking Format Preview window.
- ❑ **Ok** the Properties window.
- ❑ The main window will now show the updated Marking Format:

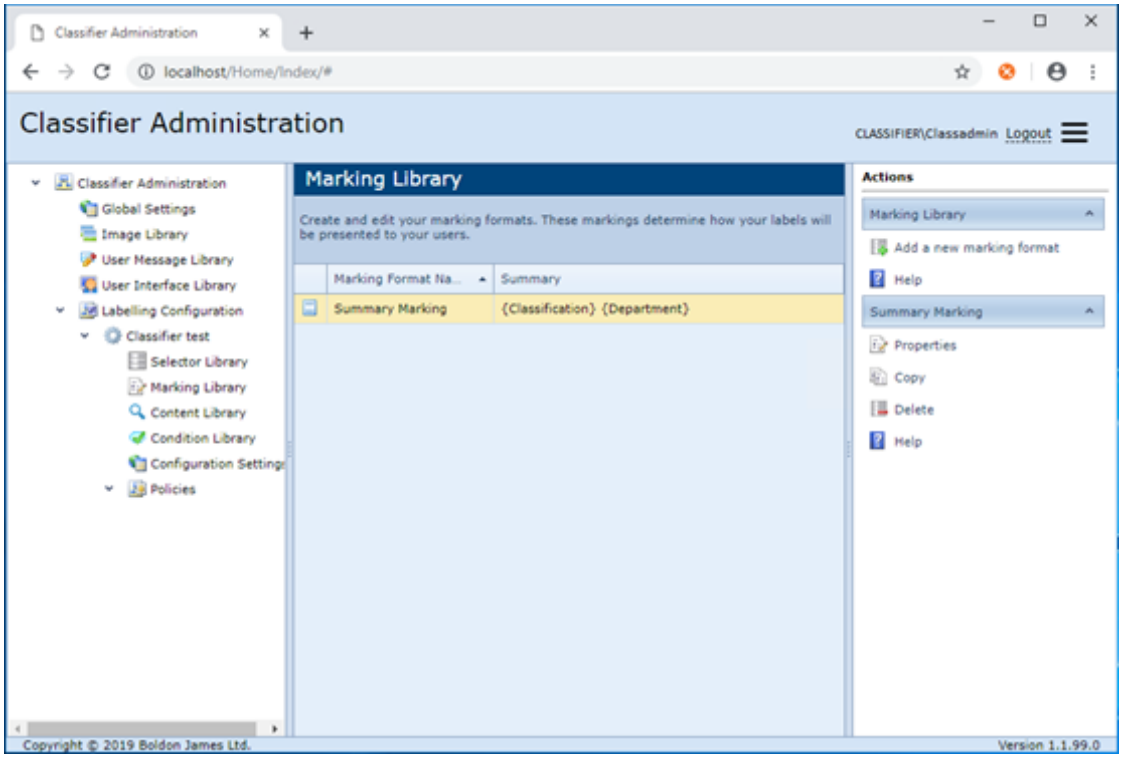


Figure 19: Marking Format Summary

3.4.2 Configure the Standard Marking Format

- ❑ Select the **Marking Library** node.
- ❑ Select the Summary Marking entry. Choose **Copy**. This adds a new entry as follows:

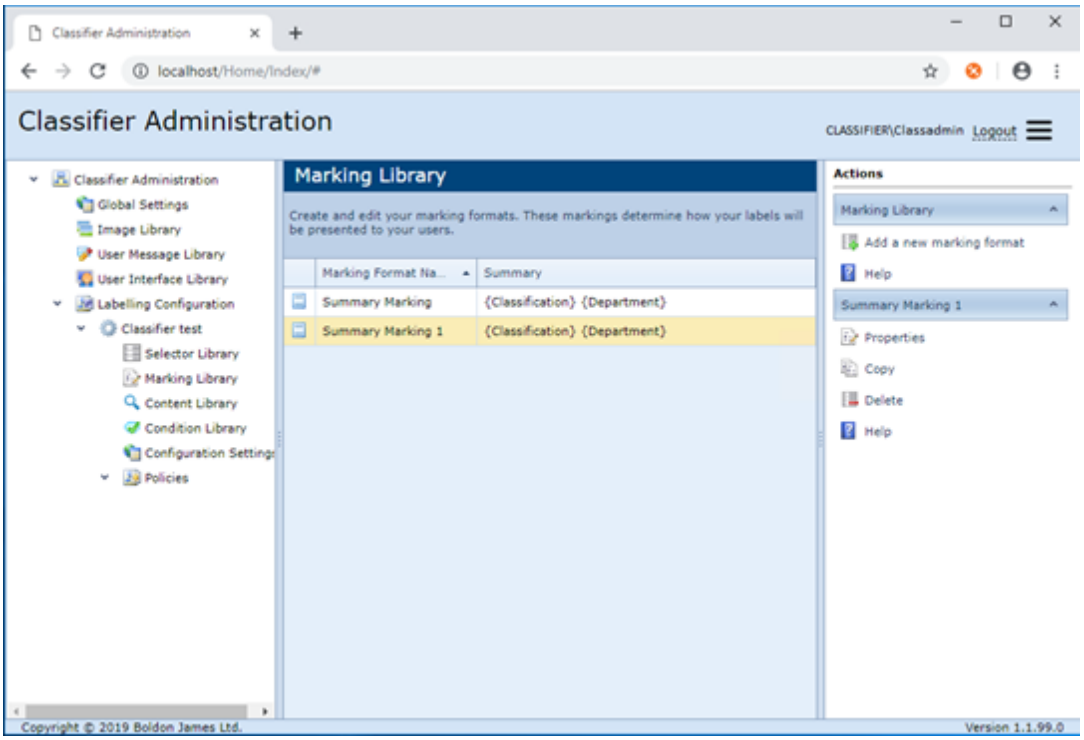


Figure 20: Summary Marking - Copy

- ❑ Select the new entry and choose **Properties**. This presents the following:

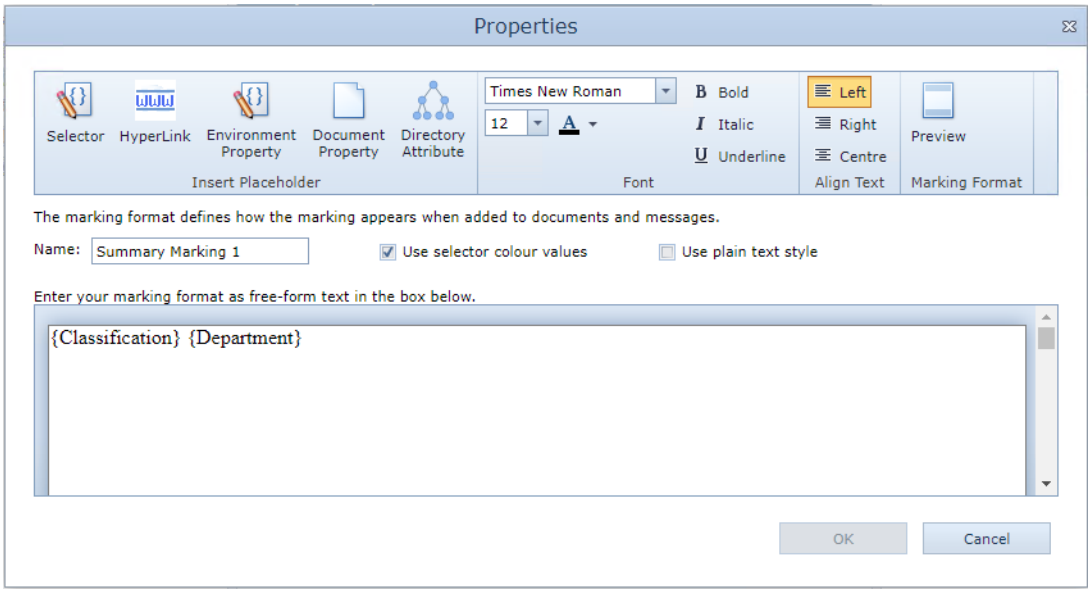


Figure 21: Summary Marking – Copy Properties

- ❑ Change **Name** to **Standard**.
- ❑ Position the cursor before **{Classification}** and click **Selector**. Select **Configuration Name** from the presented list and click **OK**. Insert a '**Space**' to leave the following:

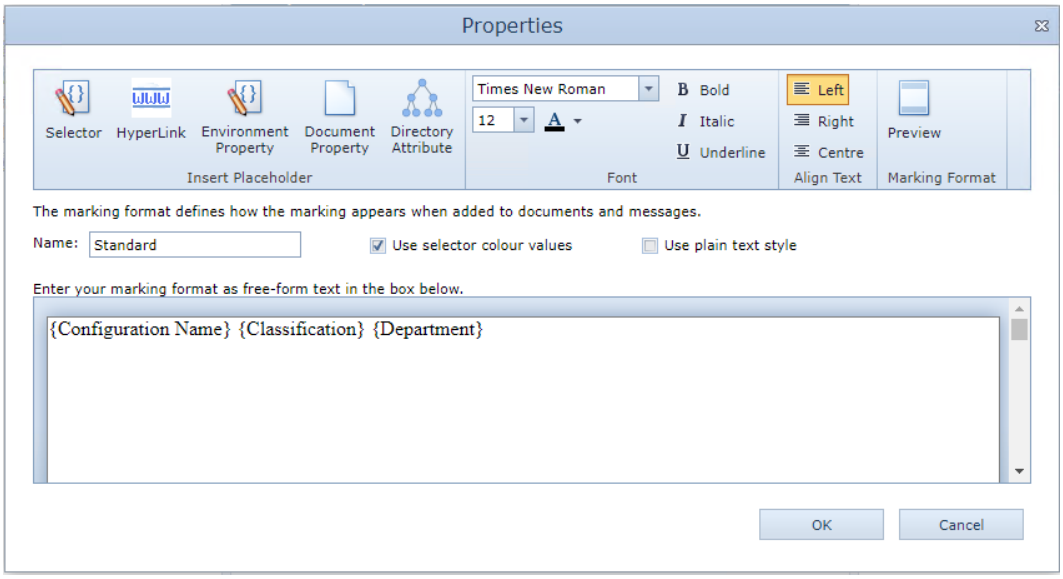


Figure 22: Standard Marking Format

Note: In this evaluation exercise, the {Configuration Name} appears so that 'externally visible' markings indicate the 'source' of the label. This might include your organisation's name for example rather than Classifier test.

- ❑ Click **OK** to save the changes and leave the summary list as follows:

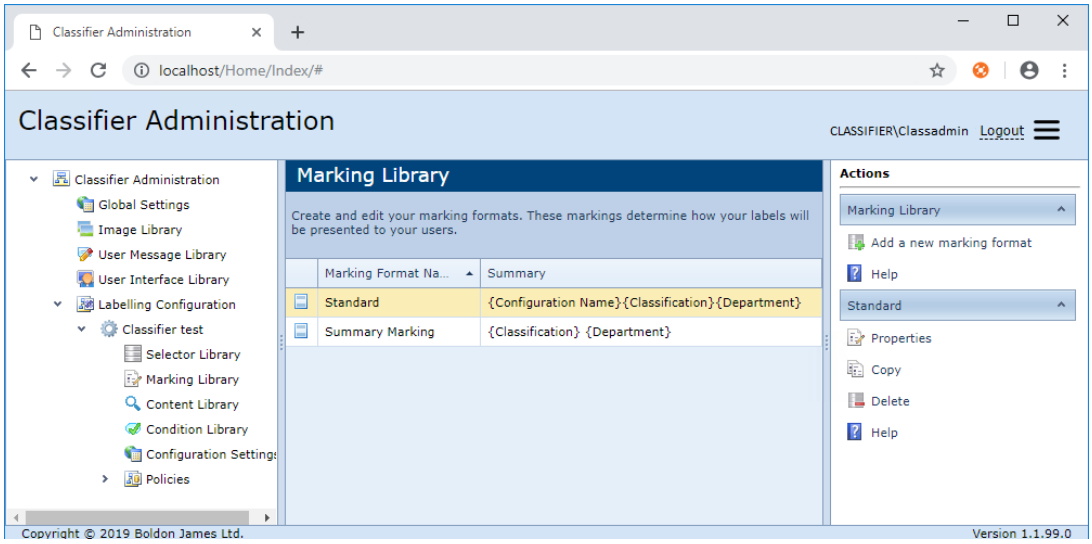


Figure 23: Marking Formats

3.5 Defining a Policy to deploy to users

Users see the Classifier Configuration through a Policy. Different users may use different policies and thereby see different views. You must define at least one Policy even if all users are to have the same view of the configuration. This section shows how to establish a Policy and configure some of the policy features.

- ❑ Select the **Policies** node and then choose **Add a new policy…**. The following will be displayed:

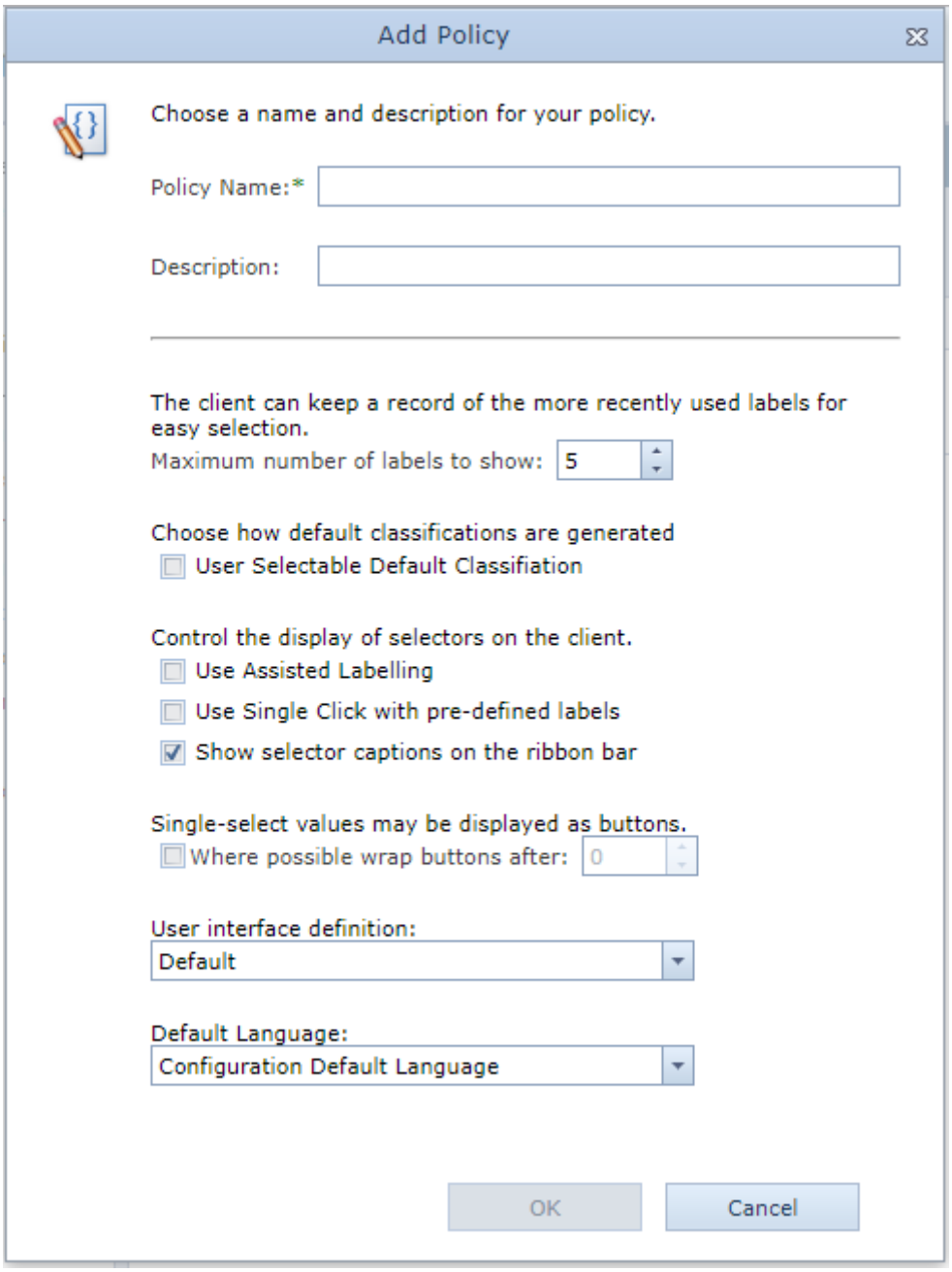


Figure 24: Defining a Policy

- ❑ Enter a Policy name of **All users**. The Description field is optional and is only relevant to the Classifier Administrator. Leave the **User interface definition** as default (the only one defined in this scenario).
- ❑ Click **OK**. The new policy will appear below the **Policies** node.

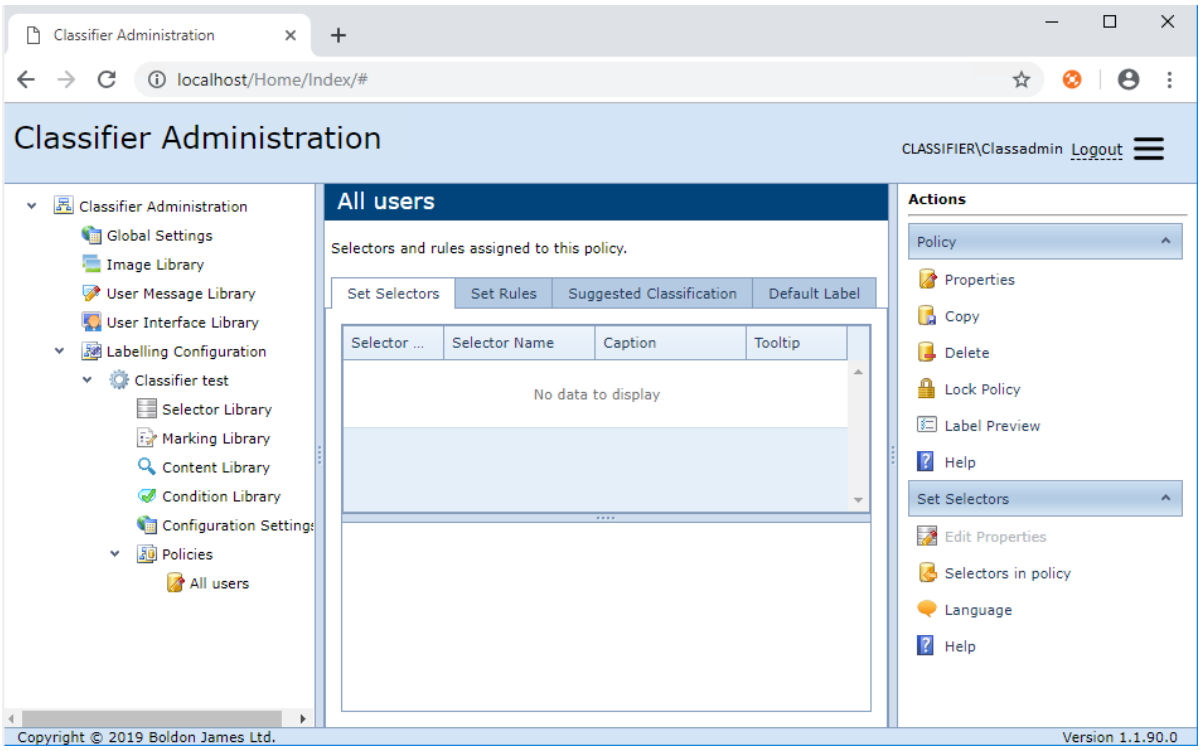


Figure 25: All users policy

3.5.1 Defining which Selectors are available in the policy

- ❑ Select **All users** from the Policies sub-tree and the middle pane presents four tabs (as per Figure 25 above).
- ❑ Select the **Set Selectors** tab in the middle section of the window and choose **Selectors in policy**.
- ❑ This will present a list of Selectors that you can assign to the policy.

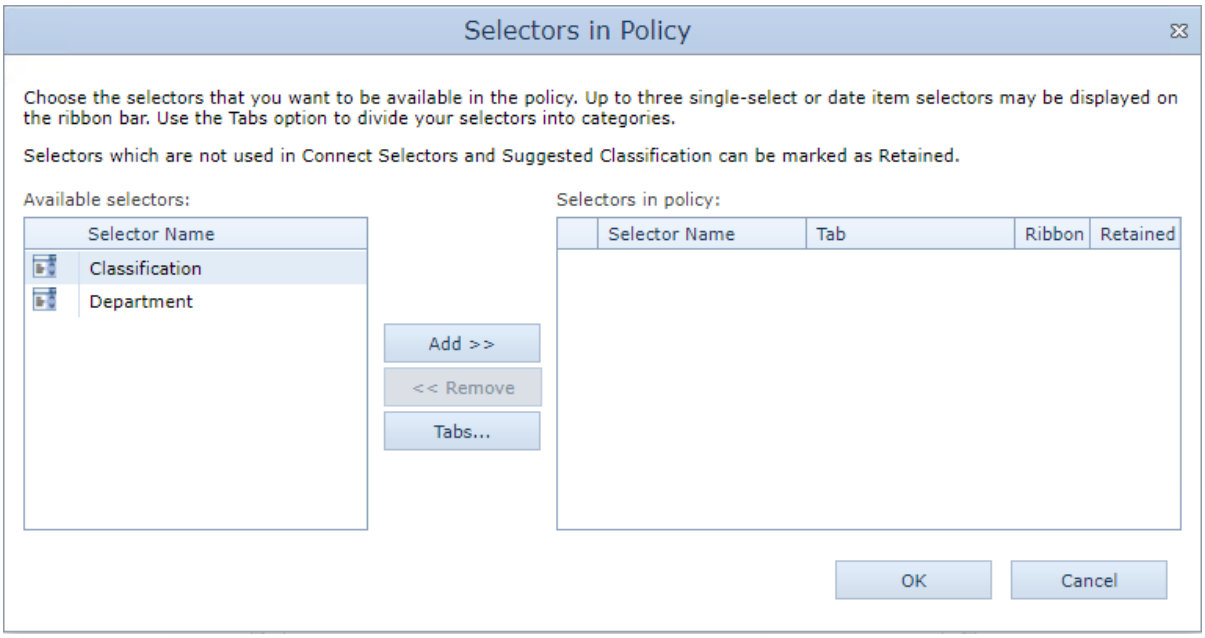


Figure 26: Set Selectors in Policy

- ❑ Select **Classification** and **Department** in turn and click **Add** for each one. Click **OK**.

- ❑ Adding a Selector to a policy also adds all of the Selector values. It is possible to remove individual values after adding the Selector.

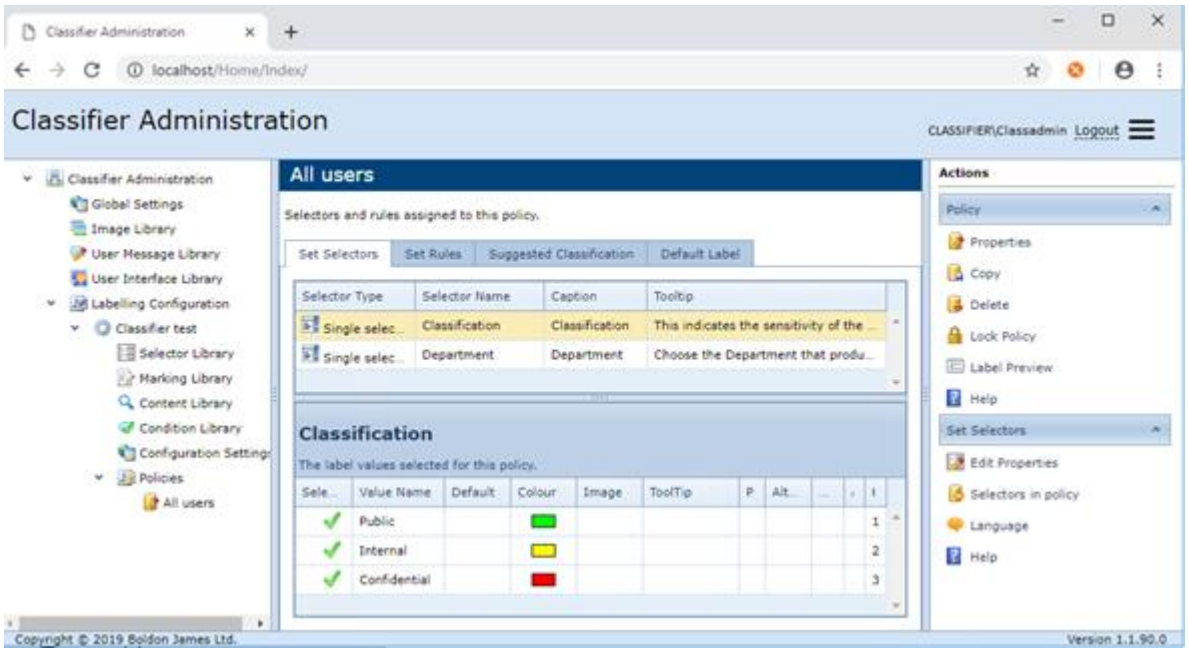


Figure 27: Classification and Values

- ❑ Classification should take a default value of **Public**. Select the **Classification** entry in the list of Selectors and choose the **Edit Properties** action.
- ❑ Select the **Options** tab.
- ❑ Select **Public** from the **Default value** drop down list.

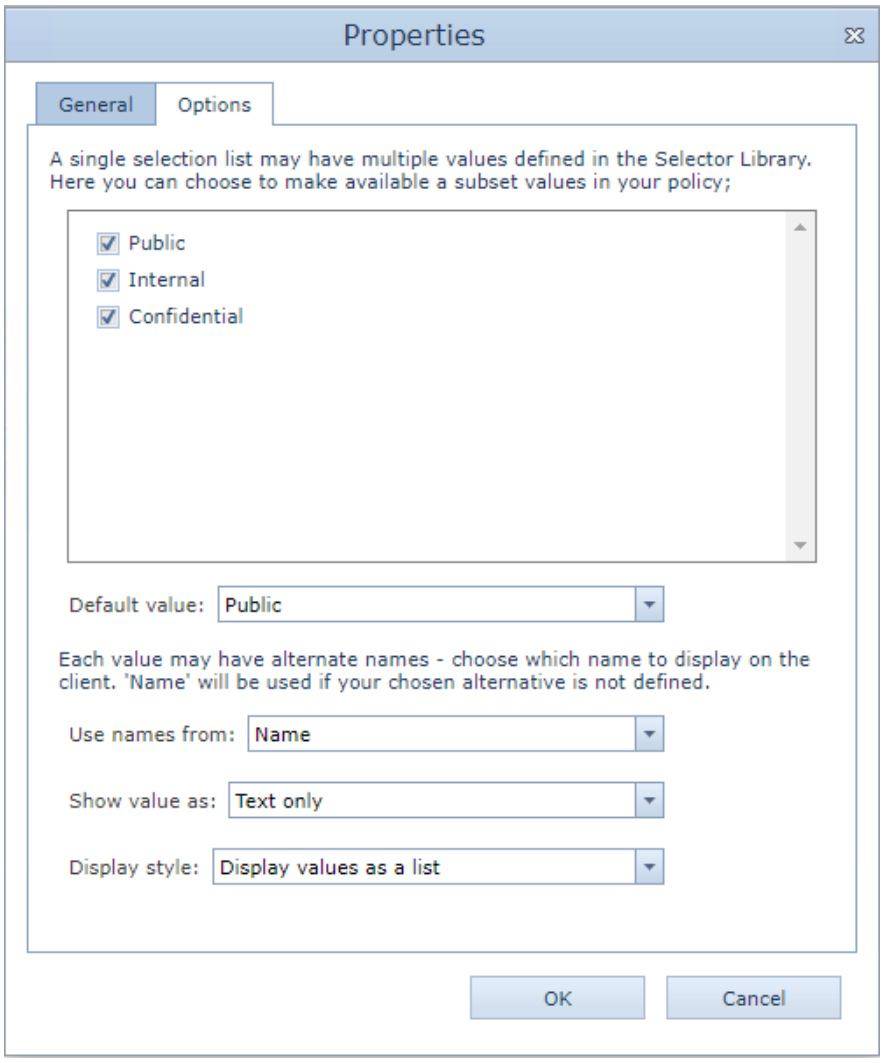


Figure 28: Selector options

- Note that we are using the Caption and ToolTip settings defined with the Selector in the Selector library. Leave **Use names from** set to Name.
- Click **OK** and the main display is updated to indicate a default is set:

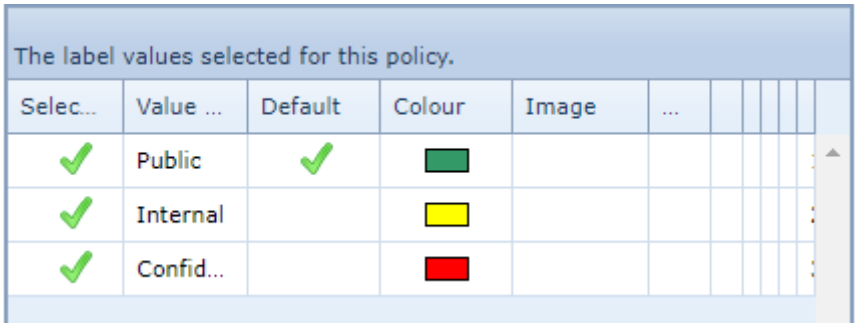


Figure 29: Classification values showing default set

3.5.2 Defining Marking Rules

The next step is to define the Marking rules that apply to documents and messages under this policy. Select the **Set Rules** tab.

3.5.2.1 Word Header Rule

- ❑ Select the **All Users** policy and select the **Set Rules** tab. The initial state is as follows:

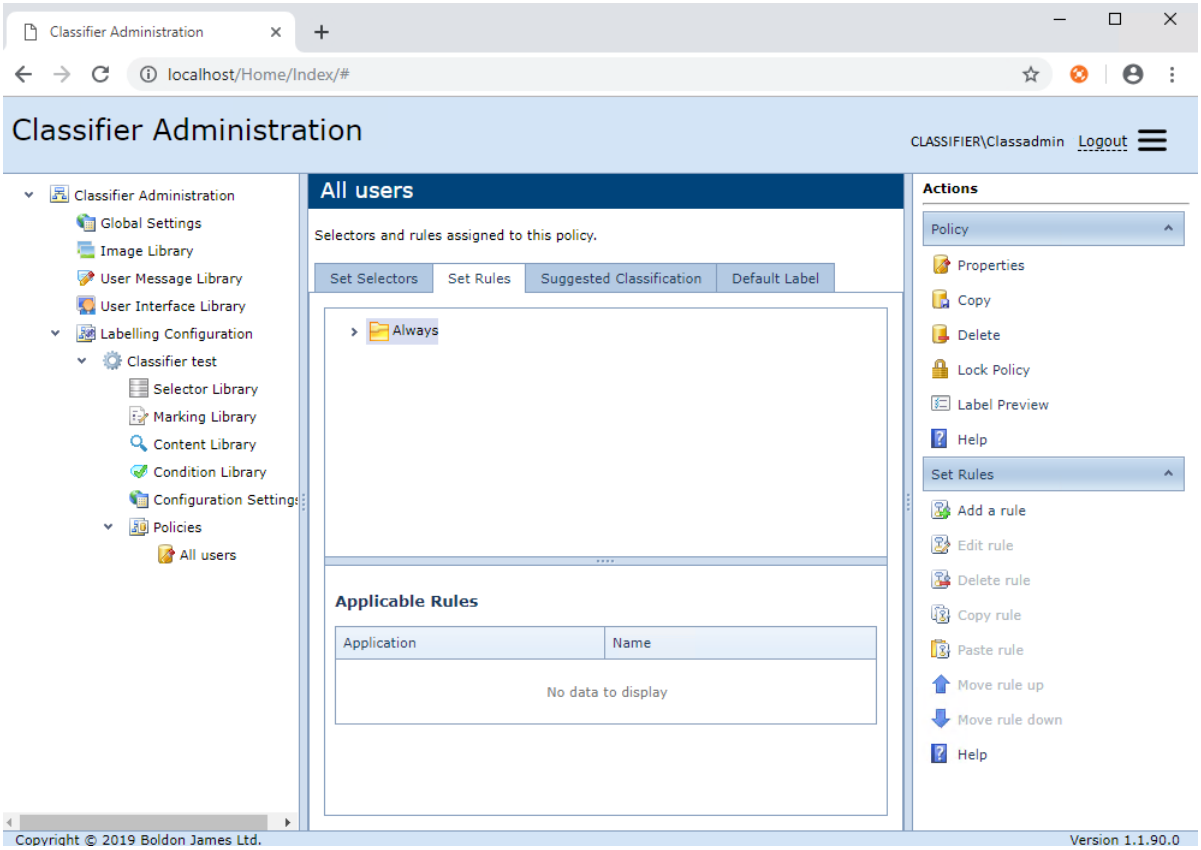


Figure 30: Rules Configuration

- ❑ Select the **Always** node and choose **Add a rule**. This starts the Edit Rule wizard:

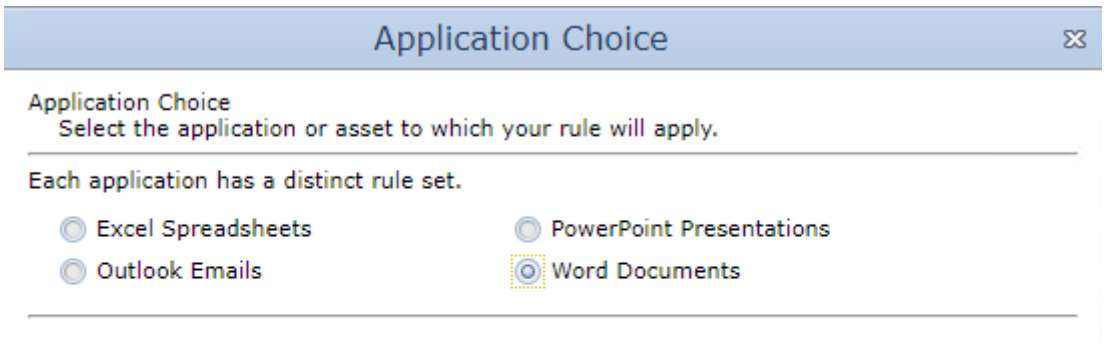


Figure 31: Choosing the Application for the Rule

- ❑ Select **Word Documents** and Click **Next**. This will present just the list of rule templates applicable to Word.
- ❑ Select the **Add a header here to any existing text in All Pages format**.

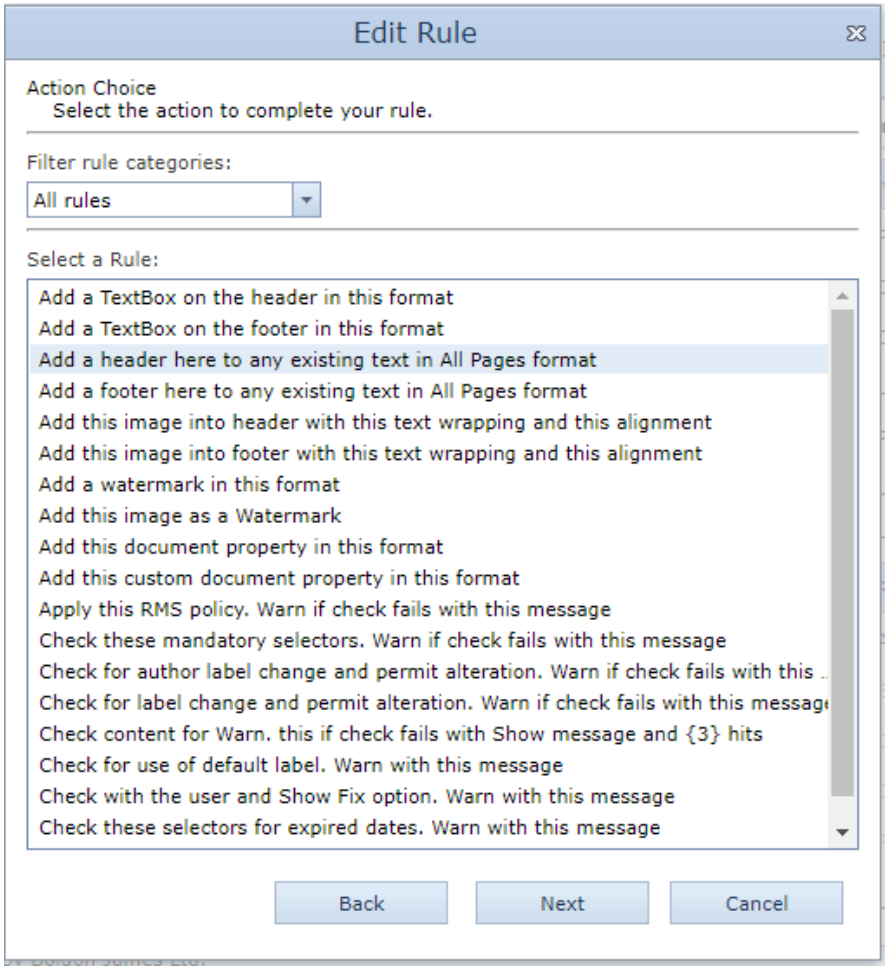


Figure 32: Add Header Marking

- Click **Next** and location and format settings dialog is presented:

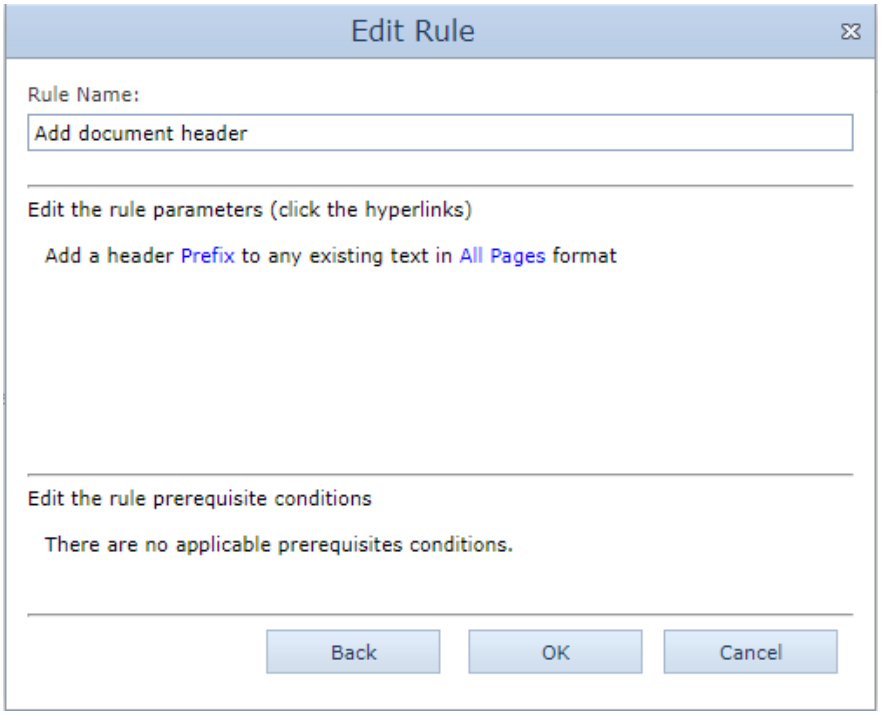


Figure 33: Add Header settings

- Select **Prefix** and it will present a choice of position. Choose **Prefix**. Click **OK**.

Figure 34: Choose Header Prefix or Suffix

- Select **All Pages** and it will present a drop down list of defined marking formats.

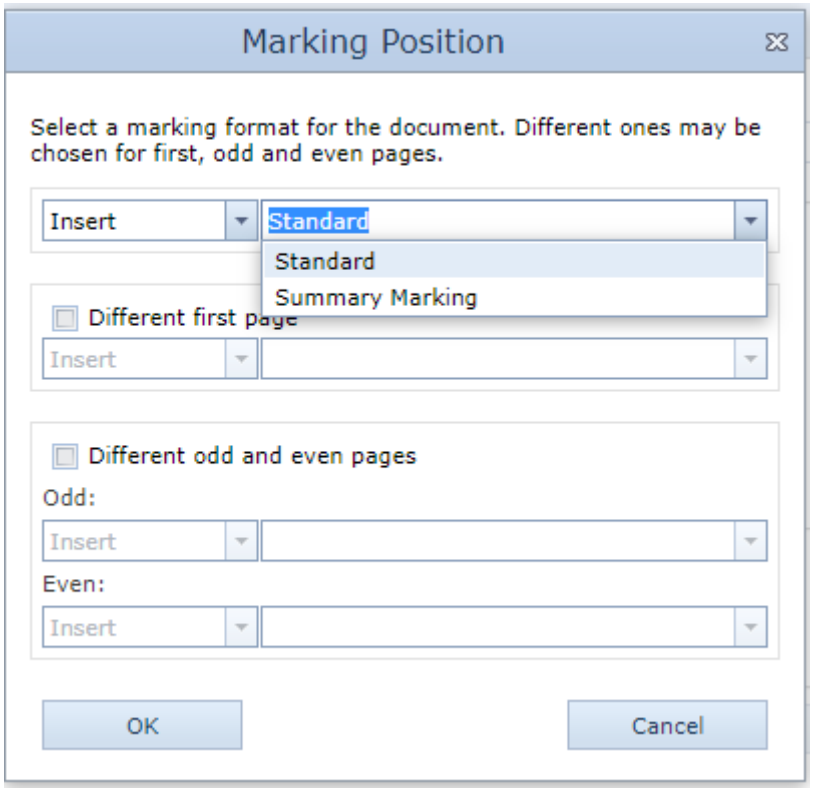


Figure 35: Use Standard Marking Format

- Select **Standard** from the drop down list and click **OK**. The **Edit Rule** dialog is updated to show:

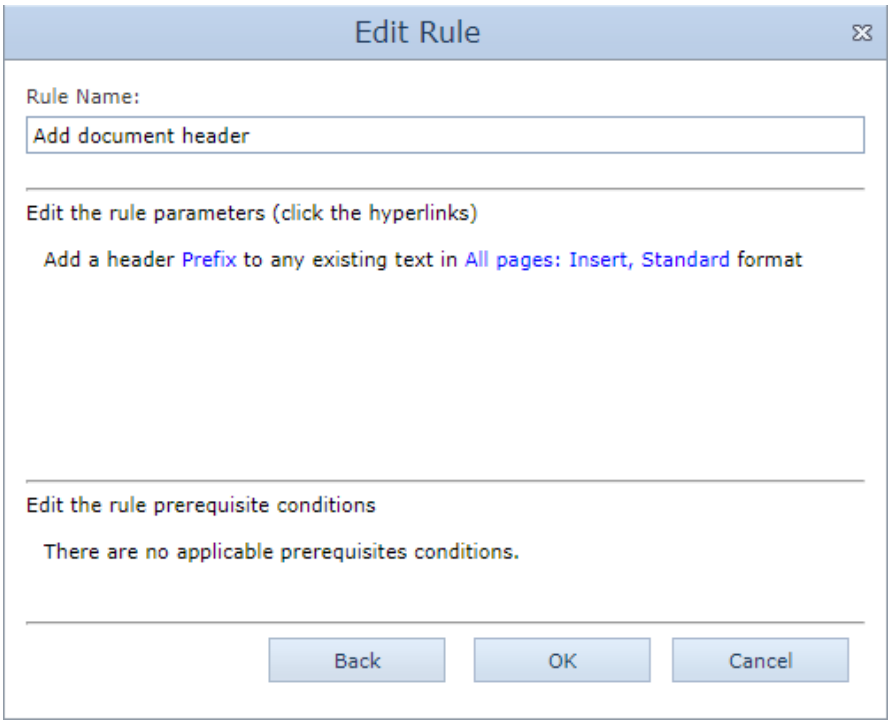


Figure 36: Configured Rule display

- ❑ Leave the **Rule Name** unchanged and click **Next**.
- ❑ If you now expand the Rules tree you will see the newly created Rule (**Add document header** - see Figure 37 below).

3.5.2.2 Word Footer Rule

- ❑ Repeat the sequence in 3.5.2.1 to establish an **Add document footer** rule –select the **Add a footer here to any existing text in All Pages format** rule this time.

3.5.2.3 Email FLOT rule

Repeat a sequence similar to 3.5.2.1

- ❑ Select **Always** and choose **Add a Rule** to launch the Rule wizard.
- ❑ This time select **Outlook emails** as the application and establish a rule based on the "**Add a FLOT in this format**"; set **this** format to **Standard** and accept the default rule name.
- ❑ This should leave you a rule summary display as follows:

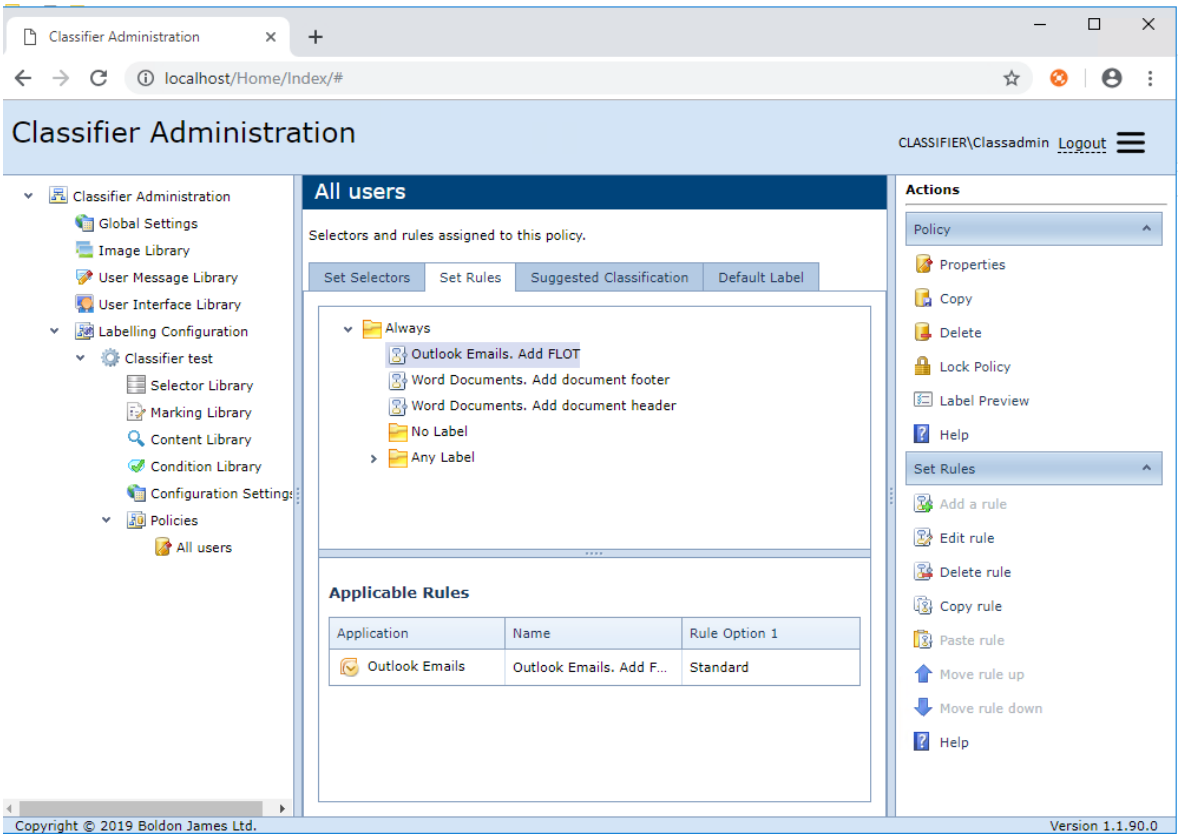


Figure 37: FLOT, Footer and Header Rules

3.6 Application and Global Settings

This test configuration uses the default Application settings found under **Configuration Settings / Classifier Application Settings** as per the example below:

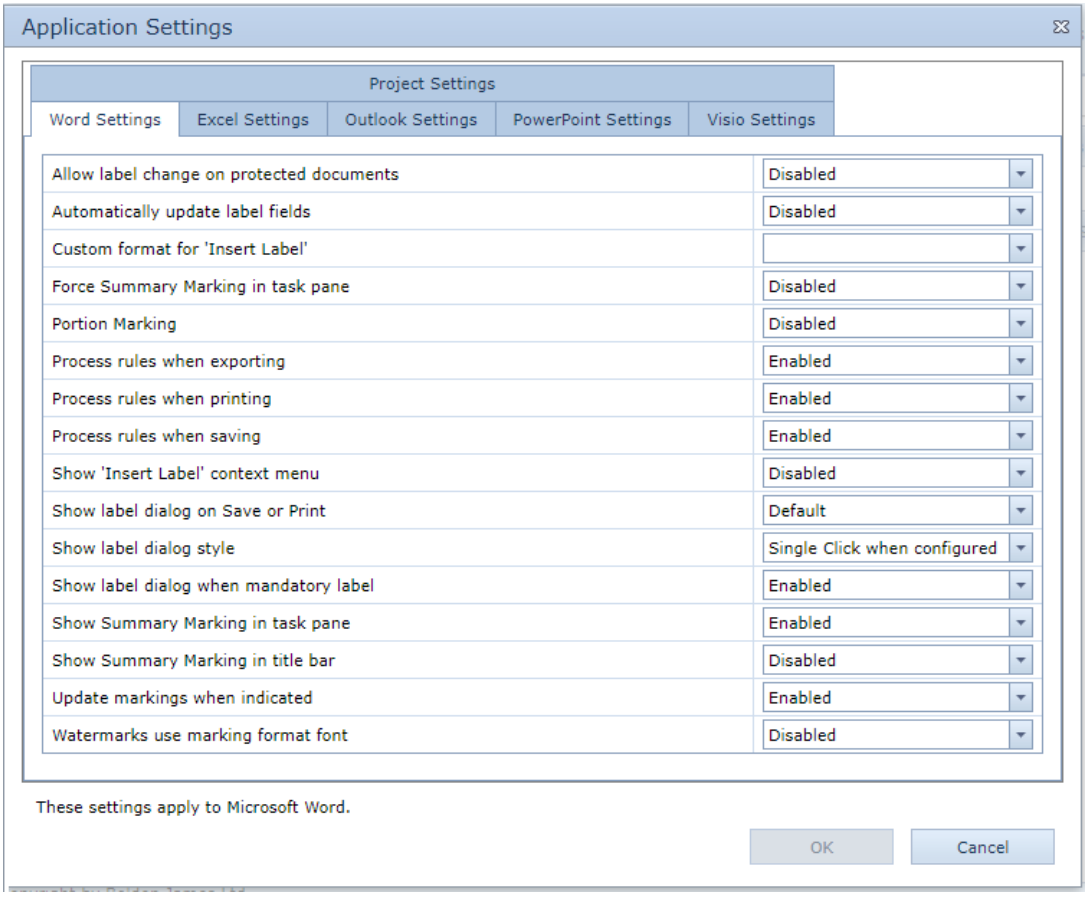


Figure 38: Classifier Application Settings

The test configuration uses the default **Global Settings** / **Application Settings**.

- ❑ Select **Global Settings** and select **Application Settings**. Choose **Properties** to show the following:

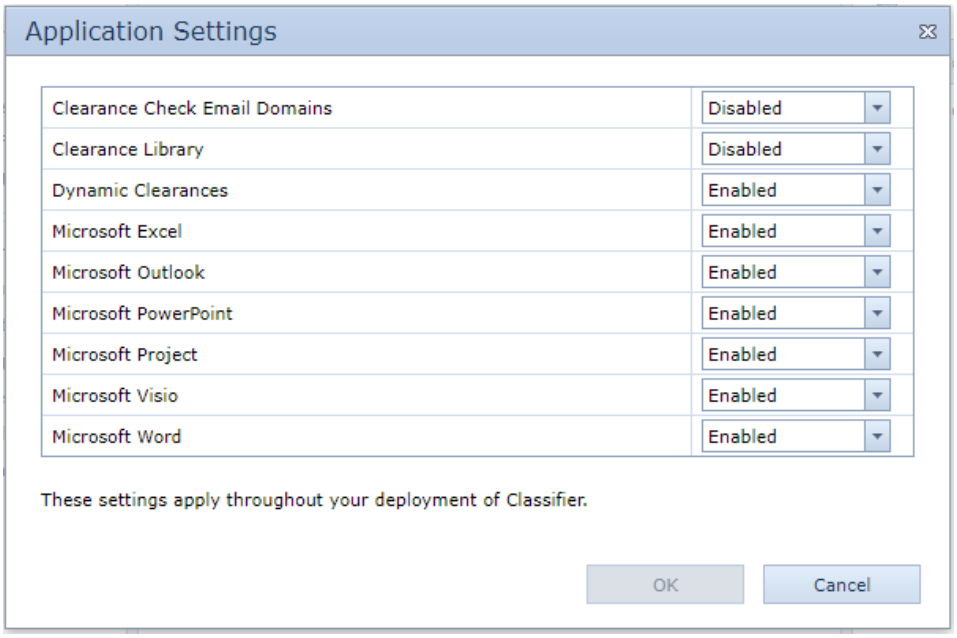


Figure 39: Global Settings Application Settings

- ❑ The basic configuration for Stage 1 is now complete.

- ❑ The next steps are to locally test the configuration and then publish the configuration to a Master Configuration location.

3.7 Locally testing the policy

Once you have completed all the configuration above you can check the effects on the client by using the **Test Mode** feature. This allows you to publish the configuration, and then run a local Test Mode Administrator application that instantiates the Test Configuration and temporarily sets a local switch that directs the Classifier Application software to utilise a 'test configuration' rather than the normal run time configuration.

On the CT-SVR-1 system:

- ❑ In Classifier Administration, select the **Classifier Administration** node.
- ❑ Choose the **Publish Test Configuration** action.

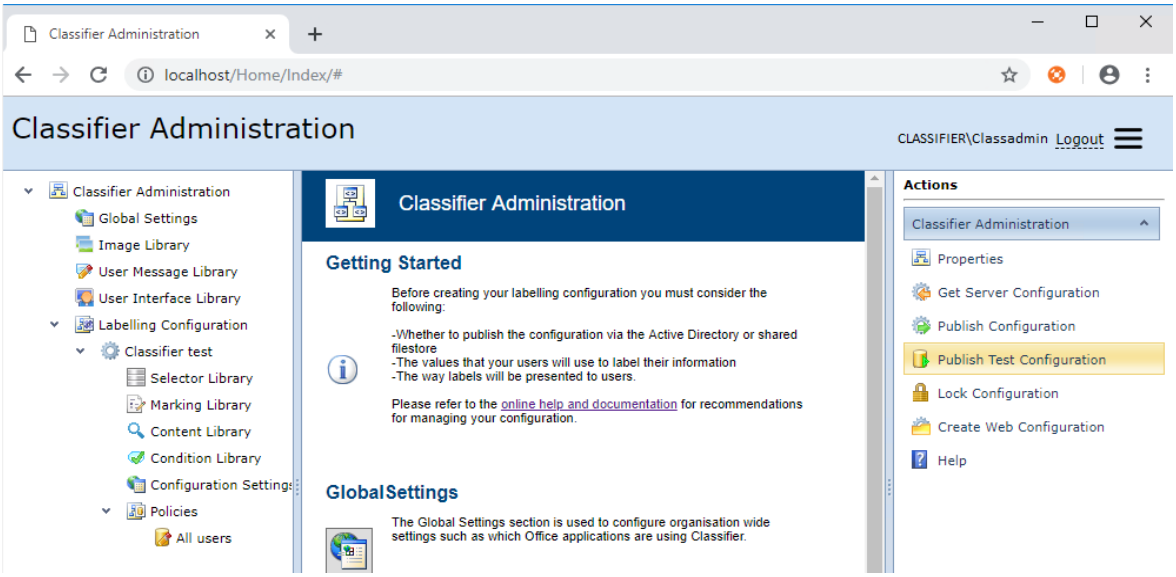


Figure 40: Publish Test Configuration

This will show the following dialog:

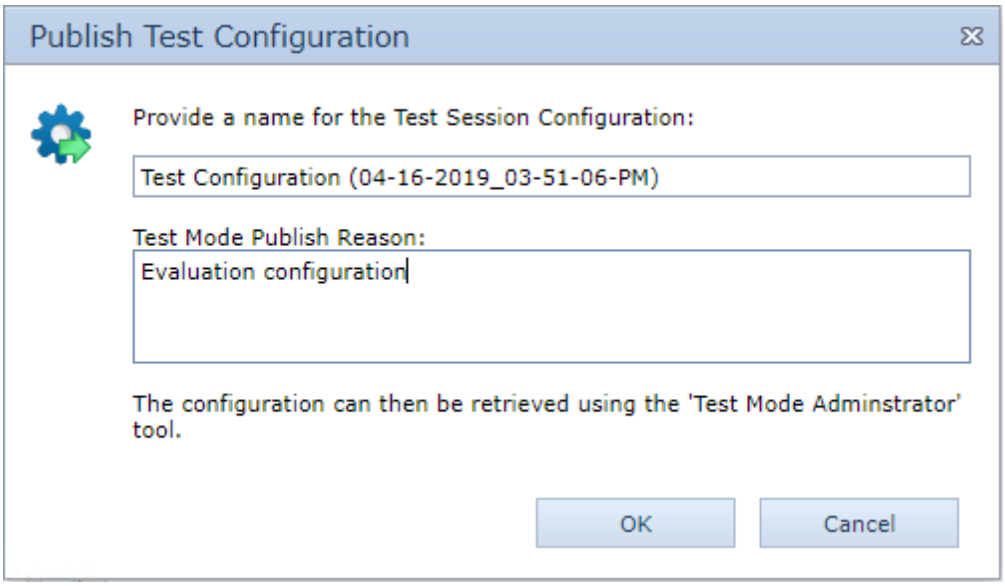


Figure 41: Test mode

- ❑ Add a reason for the test, e.g. Evaluation configuration
- ❑ Click **OK**
- ❑ By default, the test configuration will be published beneath %PROGRAMDATA% \ Boldon James \ TestMode Folder. Share this folder with the user that will be logged on to the **CT-CL-1** system.

On the CT-CL-1 system:

- ❑ Ensure that the relevant affected applications, Word and Outlook, are installed and operational.
- ❑ Ensure that none of the affected applications, Excel, Outlook, PowerPoint and Word, are running.
- ❑ Ensure that Email and Office Classifier is installed. From the Classifier Base Bundle open **Email and Office Classifier.** Choose the **x64** or **x86** folder corresponding to your Microsoft Office version and run **Setup.exe**. Follow the wizard installation steps to complete the install.
- ❑ Install the Classifier Test Mode Administration product. From the Classifier **Base Bundle** open the **Classifier Administration Server** folder and then the **Test Mode Administration** sub-folder. Run **ClassifierTestModeAdministration.msi**.
- ❑ From the Start Menu open Classifier Test Mode Administration

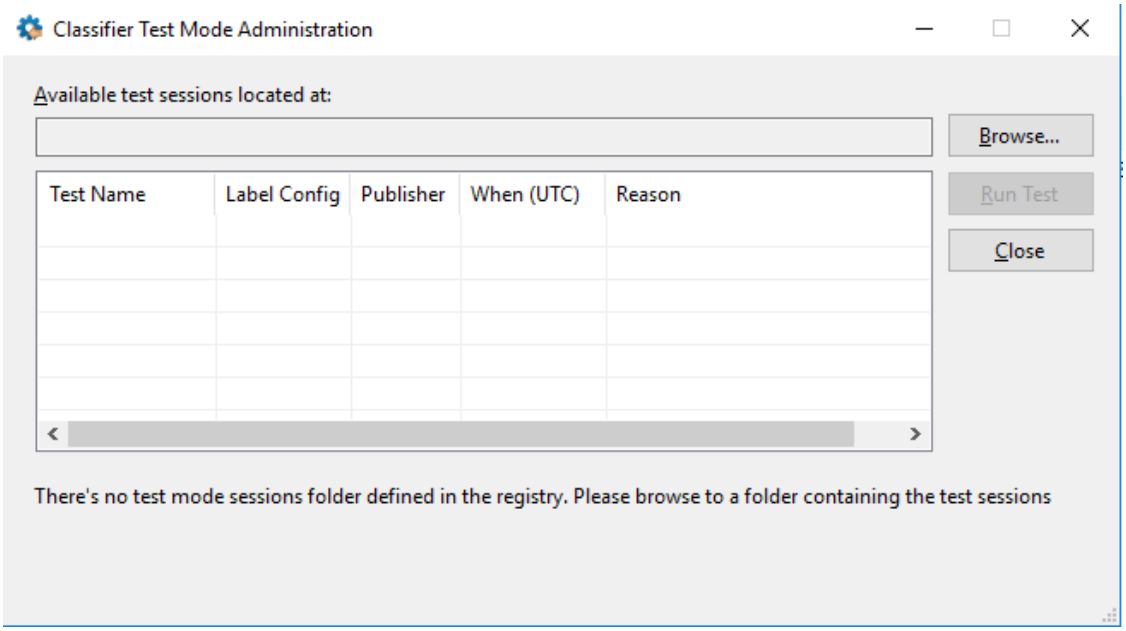


Figure 42: Test Mode Administration

- ❑ Browse to the folder shared from the **CT-SVR-1** system; that is the folder containing the published test configuration on the **CT-SVR-1** system. All test configurations published from the **CT-SVR-1** system will appear in this folder. Click **OK**
- ❑ Select the test configuration from those displayed and click **Run Test**

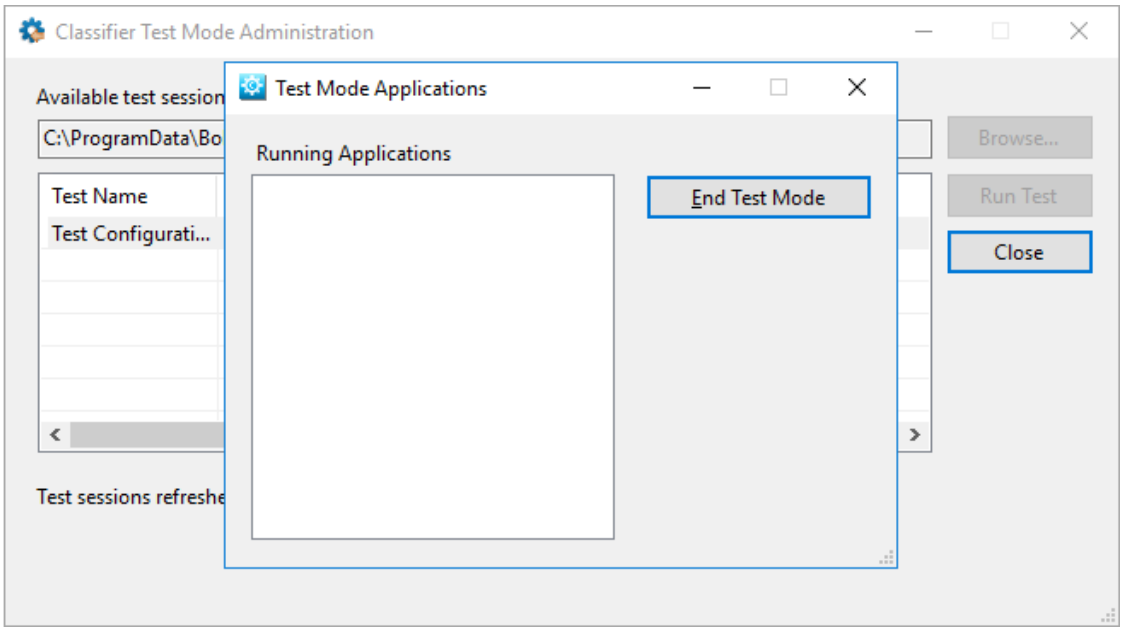


Figure 43: Test Mode Applications

- **Start** the Microsoft Office application(s) (Word and Outlook) and check the effects.
- Each time you start an application the following warning dialog appears.

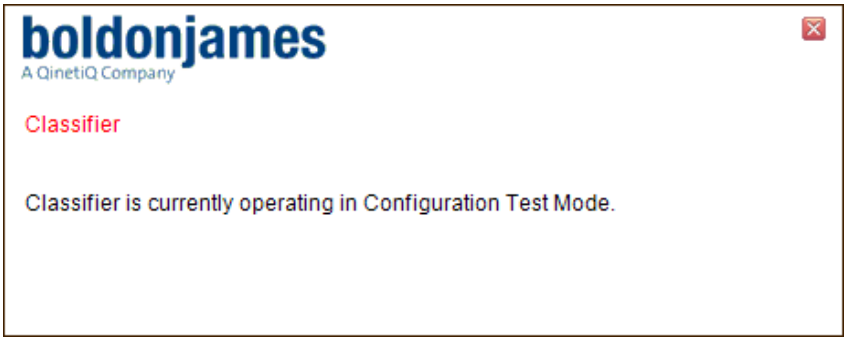


Figure 44: Test mode – Application warning

- You can now test the effects of the test configuration on the Office application. For example, in Microsoft Word with the Email and Office Classifier installed:

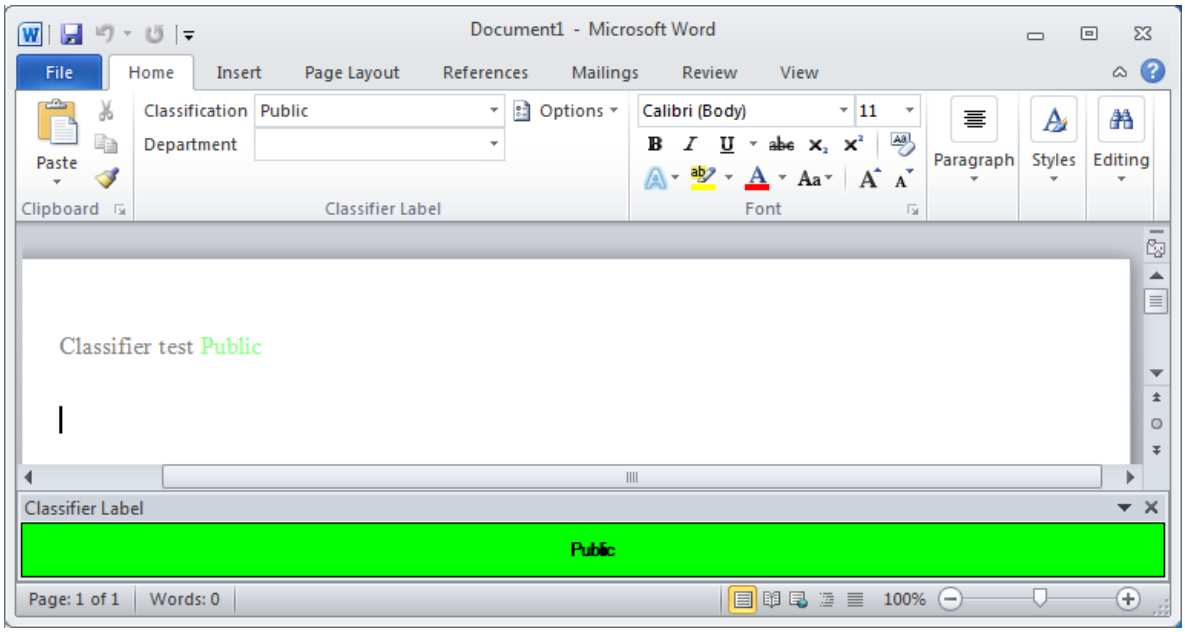


Figure 45: Word 2010 Label interface and header

- Starting Outlook and launching a **New message** will display a Classifier enabled Outlook message. The following screenshots provides examples of this. The window appearance may vary on the version of Office installed.

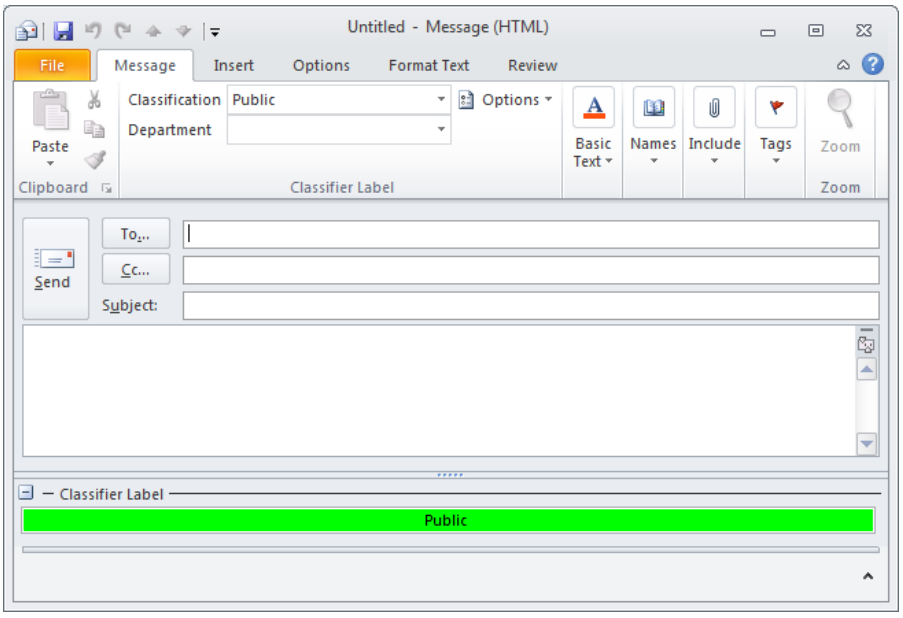


Figure 46: Outlook 2010 – Label interface and summary marking

- **Close** Outlook and Word and click **End Test Mode** on the Classifier Test Mode Administration utility. When the Office Applications, Outlook and Word, restart, they will revert to standard operation and will no longer use the Test Configuration.

3.8 Deploying the Configuration

Classifier Configuration needs to be available in every user environment. The general mechanism is described below followed by the specific actions required for this stage.

3.8.1 How the configuration reaches the client environment

Note: This section is provided for information – it contains no actions

Once the Classifier configuration is finalised, you will publish that configuration to shared File Store or to Active Directory. The schematic below shows an overview of how the configuration is deployed (full details can be found in **Classifier Administration Guide > Configuration Deployment**).

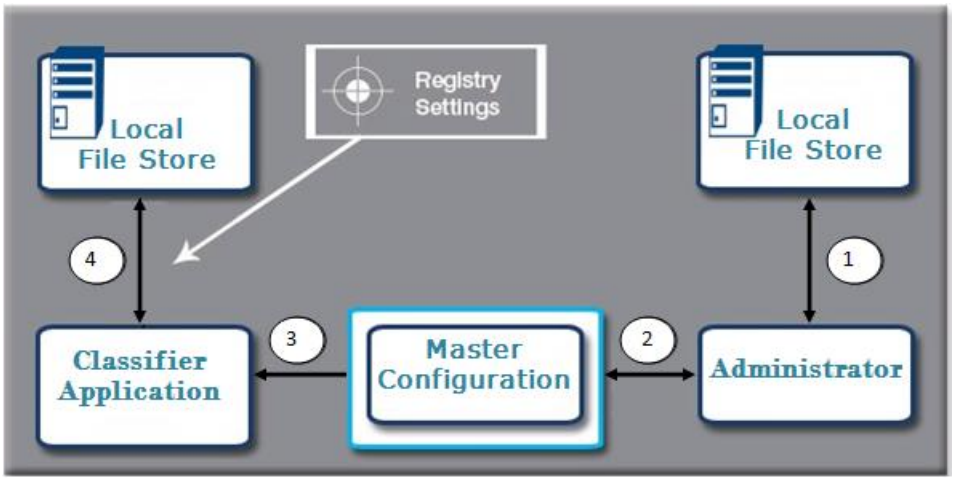


Figure 47: Configuration Deployment

Creating and Modifying the Configuration

Step 1 The process starts by the Administrator creating an initial configuration using the Classifier Administration Server and evolving that configuration to the point where it is deemed suitable for deployment to a user community. This might initially be to a pilot group or into a test environment, but might ultimately be the entire user population.

Step 2 Once the configuration is complete the Administrator will Publish the configuration to a central location. This can be the Active Directory (requires Active Directory Schema update), or a suitable shared File Store location.

When an Administrator wishes to modify the current Master Configuration they must ensure their local machine holds an up to date copy of the current Master Configuration and if necessary perform a Get Server Configuration action to retrieve the current Master - it will overwrite any prior local copy of the configuration. The administrator can then modify the Configuration and re-publish it once the changes are complete. Thus, the administrator Publishes to the Master Configuration location and the Get Server Configuration retrieves from the Master Configuration location.

Note: If you **Publish** the configuration to File Store you must ensure that the target (Master) location has suitable permissions. End users should have the ability to Read from that location and Administrators that will modify the Master configuration must have the ability to write to that location using the network path.

Classifier application retrieval of Configuration

Classifier applications need to know where to find the Master Configuration along with the **Policy** that applies to the user. The application determines this by searching registry key settings in precedence order as described in Setting the Registry Keys for this test environment (explored in section 4 of this document).

Step 3 Classifier applications, Office / Email / OWA / SharePoint Classifier / Notes Classifier, periodically retrieve the configuration. An update to the cached Configuration occurs when the Master version is newer than the local version. A **Validity Period** registry setting controls the timing of this check.

Step 4 Classifier applications will store the retrieved configuration in local file store. Clients (e.g. Email Classifier) can continue to use this local copy when operating in off-line mode.

Configuring the Client Environment

Classifier client applications needs to know the location of the Configuration information (File Store or Active Directory), and which Policy within the Configuration should be used. For further information, review Client Environment Configuration.

3.9 Publish Configuration

The next step is to **Publish** the configuration. For Stage 1 you will publish via Shared File Store.

3.9.1 Publish Configuration to File Store

- ❑ From Classifier Administration, select the top node **Classifier Administration** node and choose **Publish Configuration**.
- ❑ Select **File Store** on the dialog presented

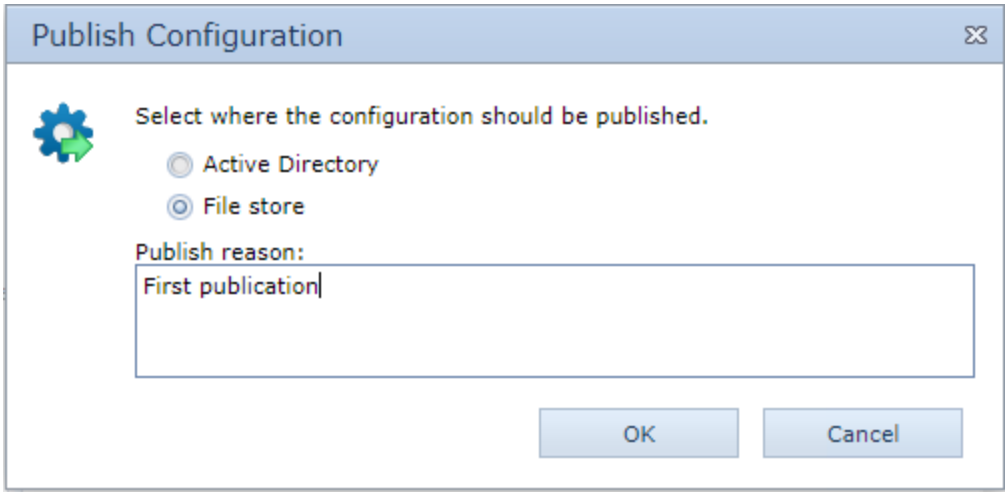


Figure 48: Publish Configuration to File Store

- ❑ Enter a reason such as **First publication** for the publication (it appears in the audit log entry). Click **OK** to complete the action.
- ❑ Click **OK** on the confirmation dialog that appears.
- ❑ The configuration is stored, by default, within the "%PROGRAMDATA% \ Boldon James \ Config Publish Folder"

3.9.2 Set the permissions to allow clients to read the configuration

- ❑ In Explorer, select the folder "%PROGRAMDATA% \ Boldon James \ Config Publish Folder**"** and then:
- ❑ Windows 2008 server:
  - Choose Share with / Specific people from the context menu.

- Add **Everyone** with **Read** permission and ensure that Administrators have **Full** control over this location so that they can publish Configuration updates.

❑ Click **OK** / **Share** / **Done** to the open dialogs to apply the changes.

4 CLIENT ENVIRONMENT CONFIGURATION

The Classifier client needs to know:

- The name and location of the configuration it should use
- The policy within the Configuration pertinent to the current user.

The client software looks for the following Registry keys (associated **Group Policy setting name** if used) holding the required information:

Name	\ServerRootType **(Configuration Distribution Server Type)**
Type	REG_DWORD
Data	0 Configuration is held in File Store (ServerFileSystemRoot key is then significant) 1 Configuration is held in Active Directory
Name	\ServerFileSystemRoot **(File Based Configuration Location)**
Type	REG_SZ
Data	(Only required if ServerRootType = 0) Path to the location that holds the Classifier Configuration folder
Key	\LabelConfiguration **(Label Configuration Name)**
Type	REG_SZ
Data	The name of the label configuration to use. e.g. Classifier test
Key	\Policy **(Policy Name)**
Type	REG_SZ
Data	The name of the policy within the configuration that this user should use. E.g. All users.

Section 4.1 describes the full set of supported Registry Key locations and their relative precedence. Section 4.2 describes which keys to set depending upon whether or not you are using Group Policy Mechanisms to manage the Registry settings.

This document describes the registry settings essential to Classifier operation. Full details of all registry settings supported can be found in **Classifier Administration > Configuration Deployment > Label Configuration Registry settings**.

4.1 Registry Key locations and precedence

[The …\Policies\.. entries are set by Microsoft *Group Policy mechanisms and should not be set directly. HKLM means HEY_LOCAL_MACHINE, HKCU means HKEY_CURRENT_USER]*

1. HKLM\SOFTWARE\Policies\Boldon James\ConfigManager\ServiceMode.
2. HKLM\SOFTWARE\Boldon James\ConfigManager\ServiceMode (only used by *OWA, SharePoint, Management Agent and CPS*). [The recommended location for services registry settings - see **Note** below the Precedence table].
3. HKCU\SOFTWARE\Policies\Boldon James\ConfigManager.
4. HKLM\SOFTWARE\Policies\Boldon James\ConfigManager.
5. HKLM\SOFTWARE\Boldon James\ConfigManager.
6. HKCU\SOFTWARE\Boldon James\ConfigManager.

Each application (Classifier Client, Classifier Administration, Notes Classifier etc.) will look for the configuration settings below these registry locations in descending order of precedence as shown in the table below.

Setting	Client	OWA	Administration Server
ServerRootType	3, 4, 5	1, 2, 4, 5	6
ServerFileSystemRoot	3, 4, 5	1, 2, 4, 5	6
LabelConfiguration	3, 4, 5, 6	1, 2, 4, 5	Not applicable
Policy	3, 4, 5, 6	1, 2, 4, 5	Not applicable

Note: Further details can be found in Classifier Administration Server Guide > Configuration Deployment.

Note: For 64-bit machines that are to run 32-bit Classifier applications (e.g. Email Classifier and Office Classifier), items 1, 4 and 5 above will need registry keys establishing under ...\SOFTWARE\Wow6432Node\Boldon James\ConfigManager as well as the locations above that will be used by 64-bit applications (e.g. OWA Classifier).

4.2 Setting the Registry Keys for this test environment

Two options are available

a) Set the Registry keys using a site defined mechanism (e.g. directly)

b) Using standard Group Policy mechanisms.

You should implement the approach (Direct setting or Group Policy) that is most appropriate for your systems before proceeding to the client verification step.

4.2.1 Set the Registry keys directly

Set the following keys under HKEY_LOCAL_MACHINE\SOFTWARE\<WOW6432Node>\Boldon James\ConfigManager

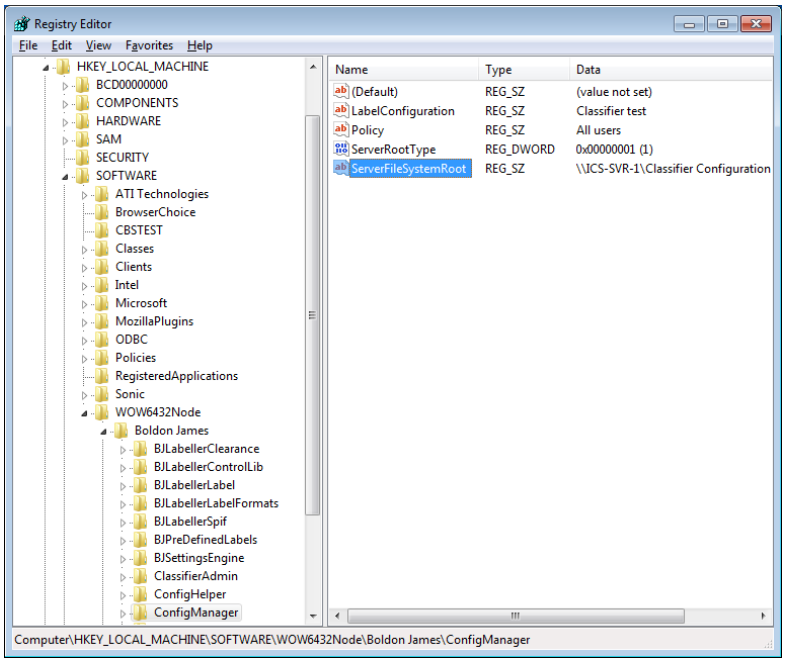


Figure 49: Local Machine Registry Keys

Remember to set the values on the clients of this test system if you wish to use the Classifier features other than through Test Mode.

4.2.2 Set the Registry keys using Group Policy

There are various ADM and ADMX files located in the **Classifier Group Policy Templates** sub-folder of the **Classifier Administration Server** folder in the Classifier **Base Bundle**. These are for use in extending the group policy settings. The two listed below are relevant to Classifier Client configuration:

- ClassifierConfig.ADM
- ClassifierConfigPerUser.ADM

The precise actions may vary depending upon your local system. The following steps apply to the evaluation scenario, which assumes that all users will use the same Policy (All users).

First, apply the Group Policy extensions. The precise sequence will depend on your specific test environment.

- ❑ Navigate to Computer Configuration.
- ❑ Use the Group Policy Management Editor MMC snap-in to get directly to the target **Default Domain Policy** tree and choose **Edit…** from the context menu.
- ❑ Select **Computer Configuration/<Policies>/Administrative Templates** and select **Add/Remove Templates** from the context menu.
- ❑ Select **Add** and then browse to the install locations (e.g. **Program files\Boldon James\Classifier Administration**)
- ❑ Select the **two ADM files** and click **Open** followed by **Close**. The files add new entries below both the Computer Configuration and User Configuration Administrative Templates nodes.

You are now ready to apply Classifier control settings to ensure that the client products will obtain their configuration from the correct location and that users see the **All Users** Classifier policy.

- Select **Computer Configuration / <Policies> / Administrative Template / (Classic Administrative Templates) / Boldon James / Label Configuration** which will present the following settings:

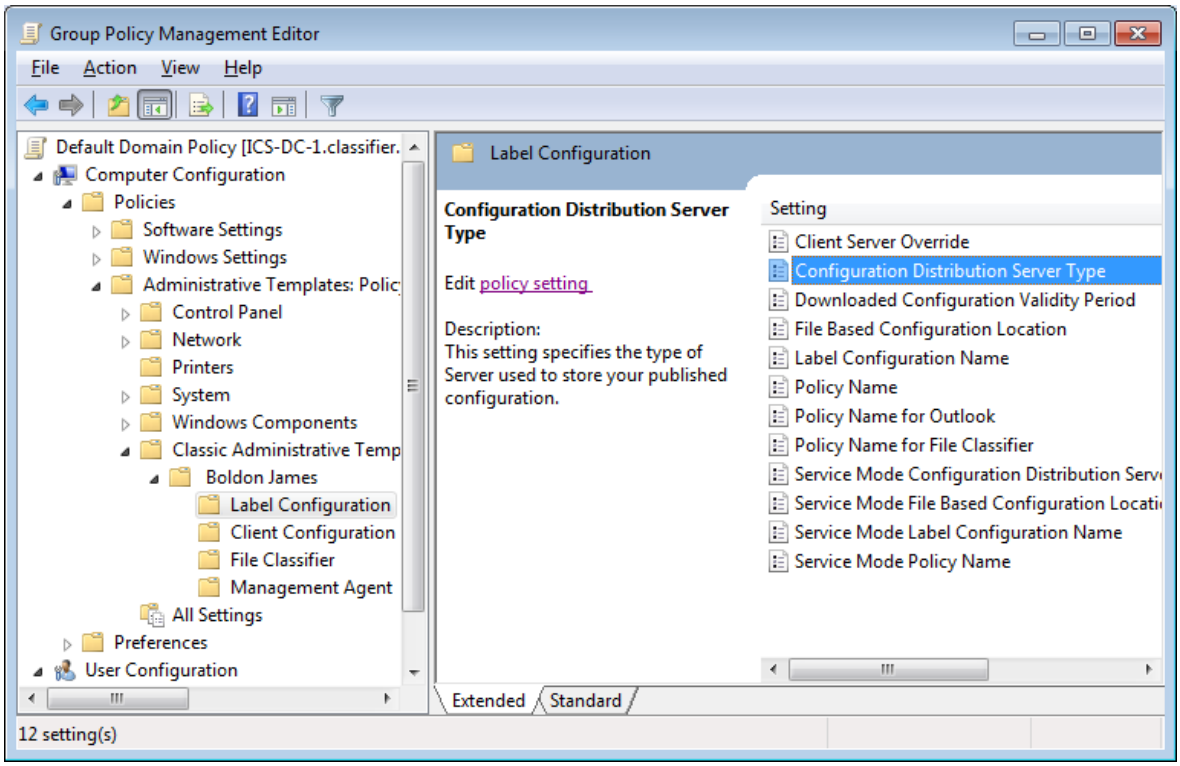


Figure 50: Set Configuration Distribution Server Type

- Select Configuration Distribution Server Type and choose **Edit Policy setting**.

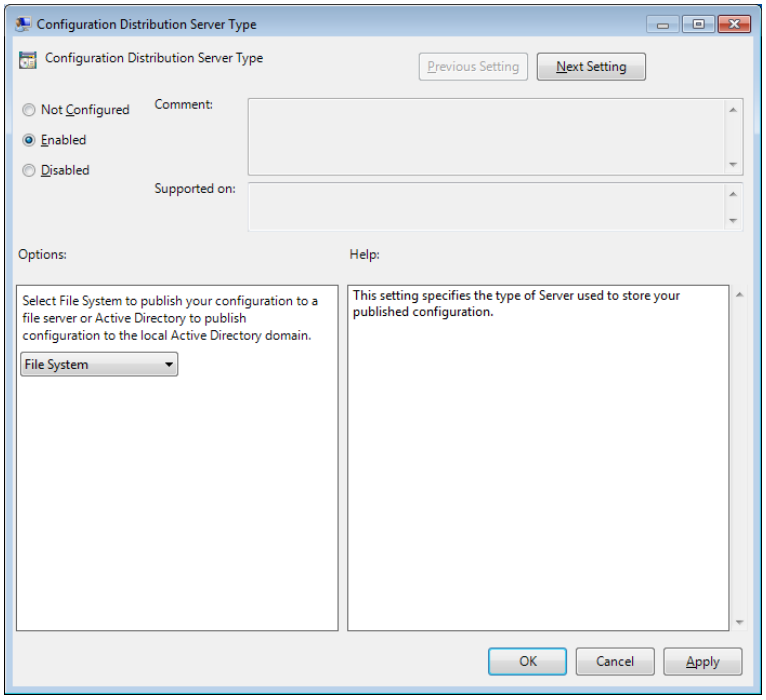


Figure 51: Enable Configuration via File Store

- Select **File System** from the drop down and click **Enabled**. Click **OK**

- ❑ Select **File Based Configuration Location** and choose Edit **Policy setting**
- ❑ Enter the master configuration folder (**\\CT-SVR-1\Classifier Configuration**).

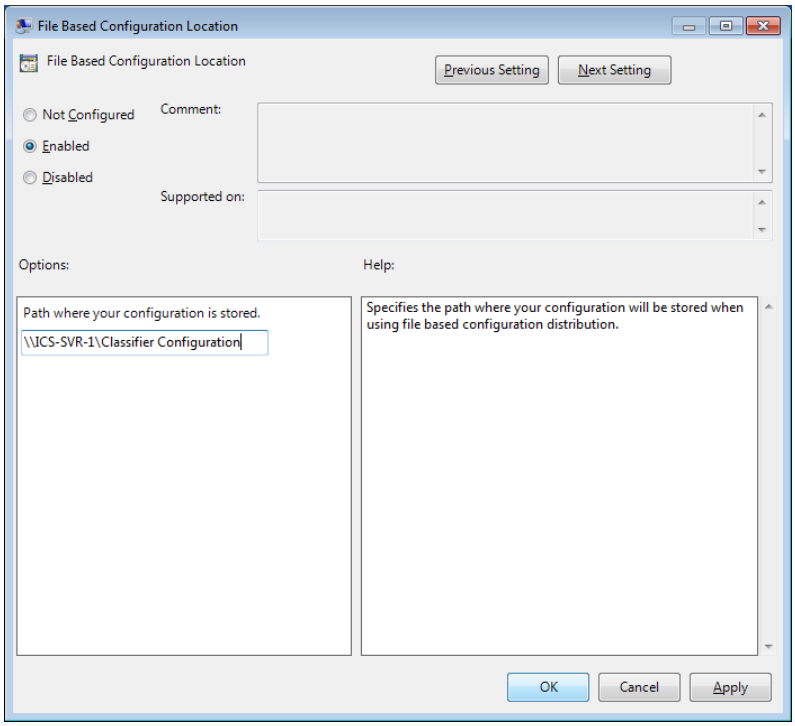


Figure 52: Set location of Master Configuration (2008)

- ❑ Click **OK**.
- ❑ Now for the Current User settings – Select **User Configuration / <Policies> / Administrative Template / (Classic Administrative Templates) / Boldon James / Label Configuration**.

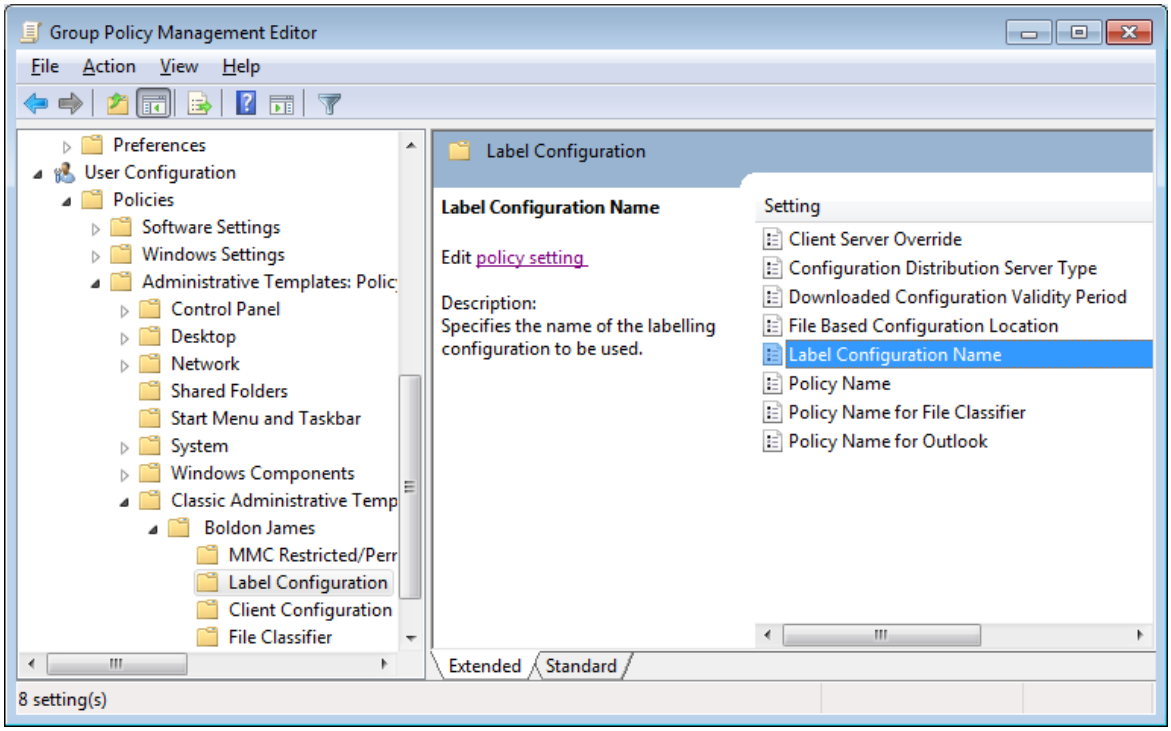


Figure 53: User Policy settings

- ❑ Select **Label Configuration Name** and choose Edit **Policy setting**.

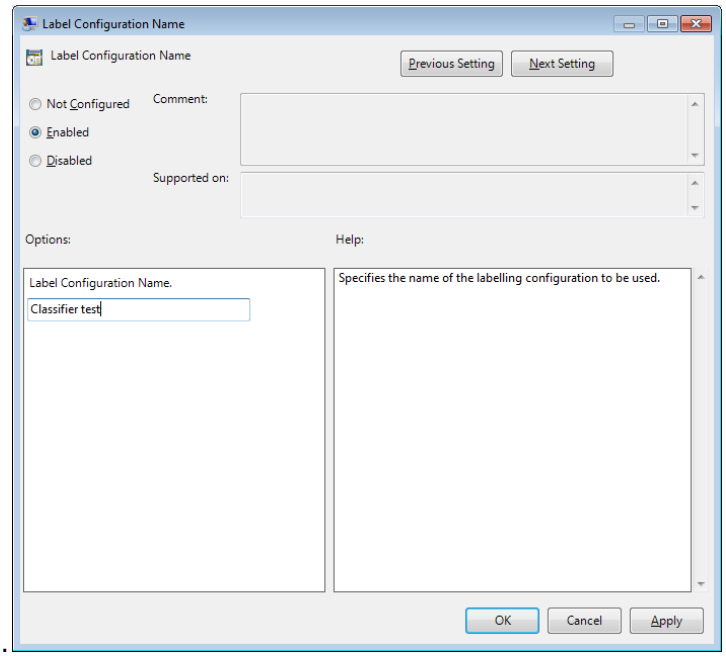


Figure 54: Label Configuration Name

- ❑ Enter **Classifier test** and click **OK**.
- ❑ Select **Policy Name** and choose **Edit** Policy setting.

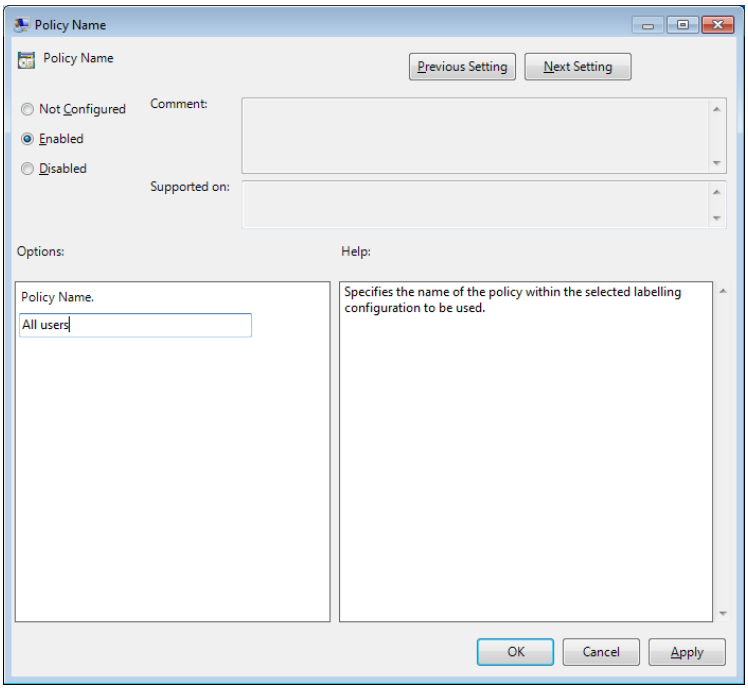


Figure 55: Policy Name

- ❑ Enter **All Users** and click **OK**.

Note: This evaluation example does not use the Downloaded Configuration Validity Period.

The next section shows the registry keys created on the client.

4.2.2.1 Client Registry Settings

Note: If you are using Group Policy and the relevant keys are not established, then running GPUPDATE /Force may be of assistance.

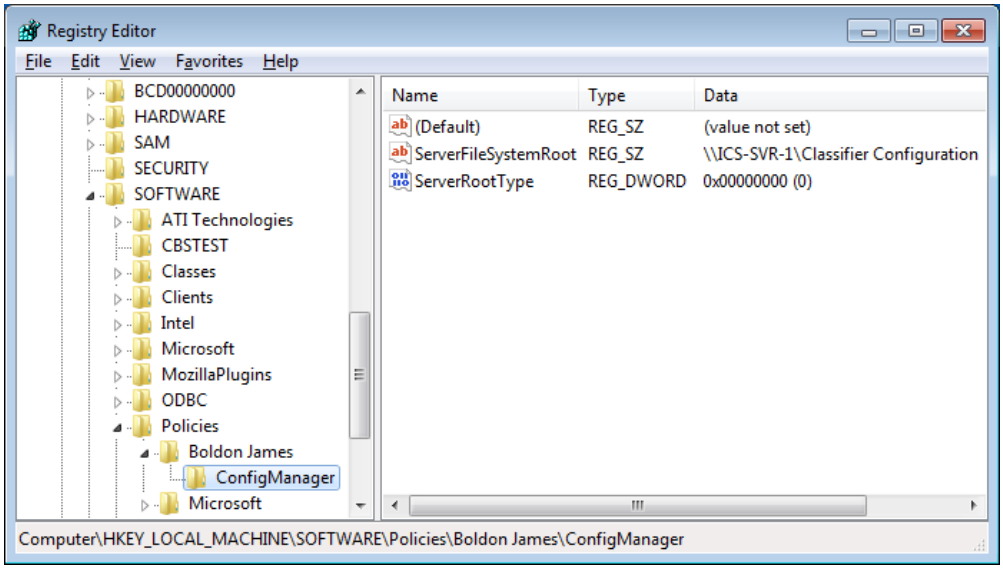


Figure 56: Local Machine settings

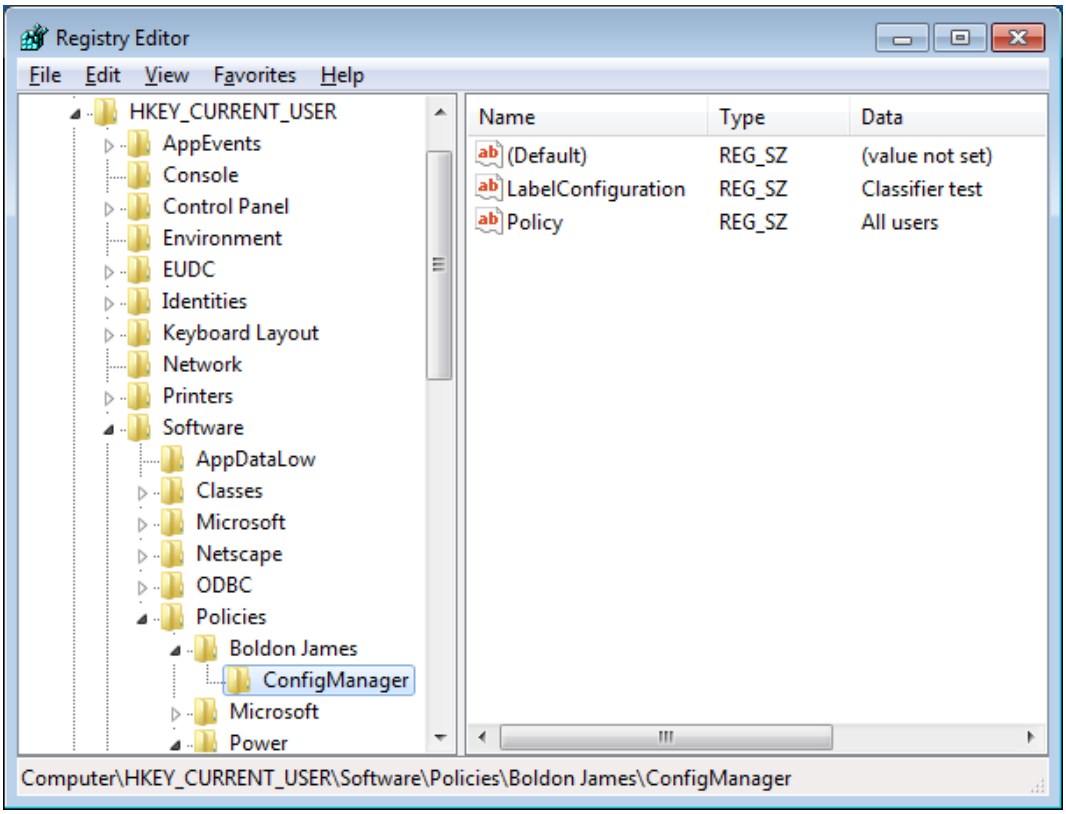


Figure 57: Current User settings

5 VERIFY INITIAL CLIENT FUNCTIONALITY

The following section describes how to install Classifier Client products onto the PCs described in section 2. (**CT-CL-1** and **CT-CL-2**, each with a test user account called **SalesUser1** and **SalesUser2** respectively).

5.1 Configure Client PC

To configure each client PC you must:

- ❑ Configure the client environments for CT-CL-1 / CT-CL-2 as detailed in section 2.
- ❑ Install the Classifier software (5.2 below)

5.2 Install Classifier

To install Classifier onto each client PC:

- ❑ Log on to the client PC as an administrator.
- ❑ From the Classifier Base Bundle open **Email and Office Classifier.** Open the **x64** or **x86** folder corresponding to your version of Microsoft Office and run **Setup.exe**.
- ❑ Follow the Classifier installation wizard steps to complete the installation.

We now need to configure the client environment to obtain the label configuration information. Setting Classifier Registry keys in accordance with section 4.2.1 or 4.2.2 directs clients to the label configuration. Ensure that the clients are re-started to pick up any Group Policy settings defined.

5.3 Confirm the installation of Classifier on the client PC

To verify the installation and operation of Classifier Client applications:

- ❑ Log onto CT-CL-1 as SalesUser1.
- ❑ Open a Word document and a new Outlook message.
- ❑ Check that a new document displays a header and footer values, and the Label selection interface.
- ❑ Check that Outlook shows the label selection interface.
- ❑ Log onto **CT-CL-2** as **SalesUser2** and repeat.

6 DEMONSTRATE FUNCTIONALITY CHANGES.

This section implements an additional Classifier feature to require users to select a Classification value when sending a message. This makes use of two additional aspects of Classifier configuration:

- Define a message for the user if they contravene the rule defined below.
- Establish mandatory selector rules for Outlook emails.

The section then demonstrates deployment of these changes to the users.

Note: Mandatory Label checks are application specific, so it is possible to demand a Classification for a message, but not require a Classification for a Word document for example.

6.1.1 Configure User Message

The template configurations include various pre-defined user messages that you can use, or modify to meet your requirements. The sequence below modifies a pre-defined message by way of example. Alternatively, you could use the **Add a new message** action to create a separate message for this purpose.

❑ Select **User Message Library** to show the list of messages.

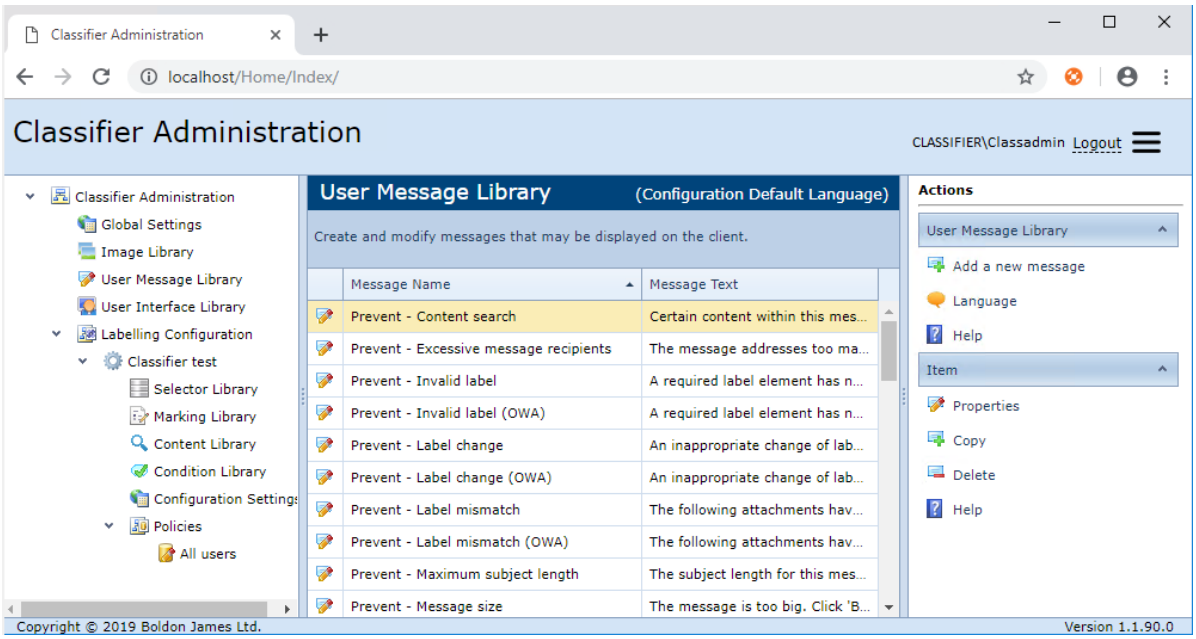


Figure 58: User Message List

❑ Select the **Prevent – Invalid label** entry from the list. Choose **Properties**. This will show the default properties.

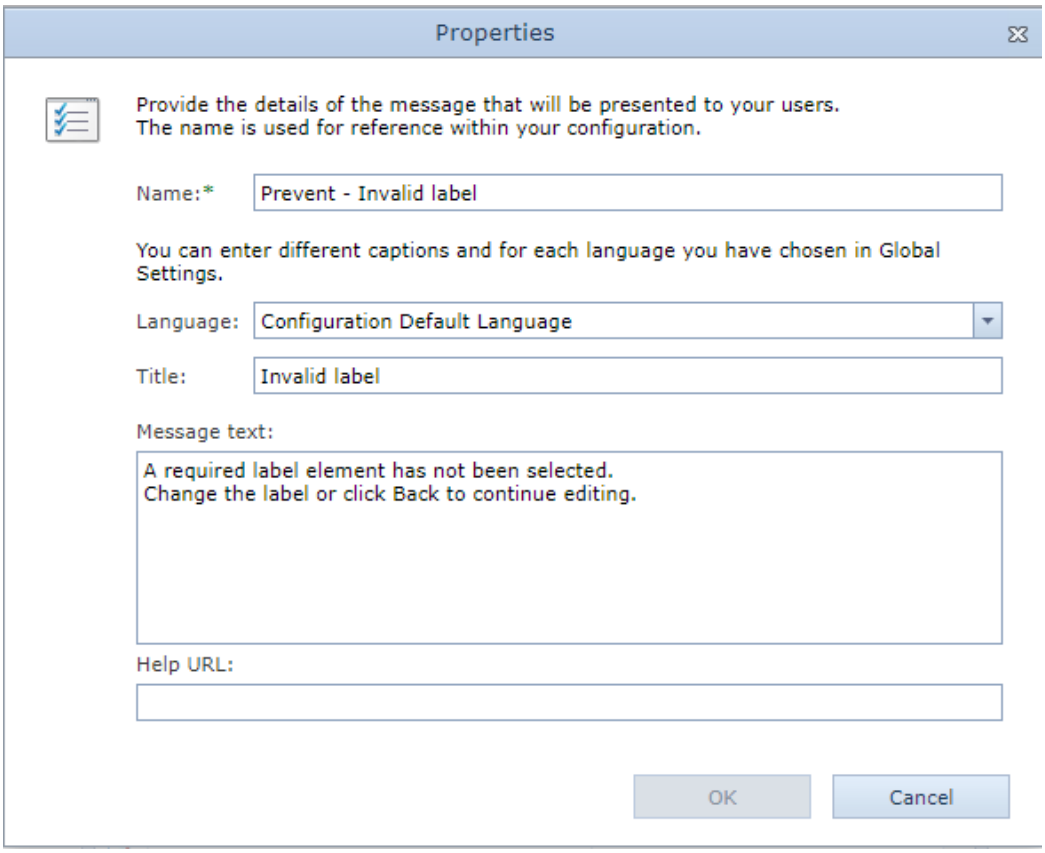


Figure 59: Prevent – Invalid label

- ❑ Change the first line of the Message text to the more specific "**You must select a Classification value**." Click **OK**.
- ❑ The message will appear in the summary list.

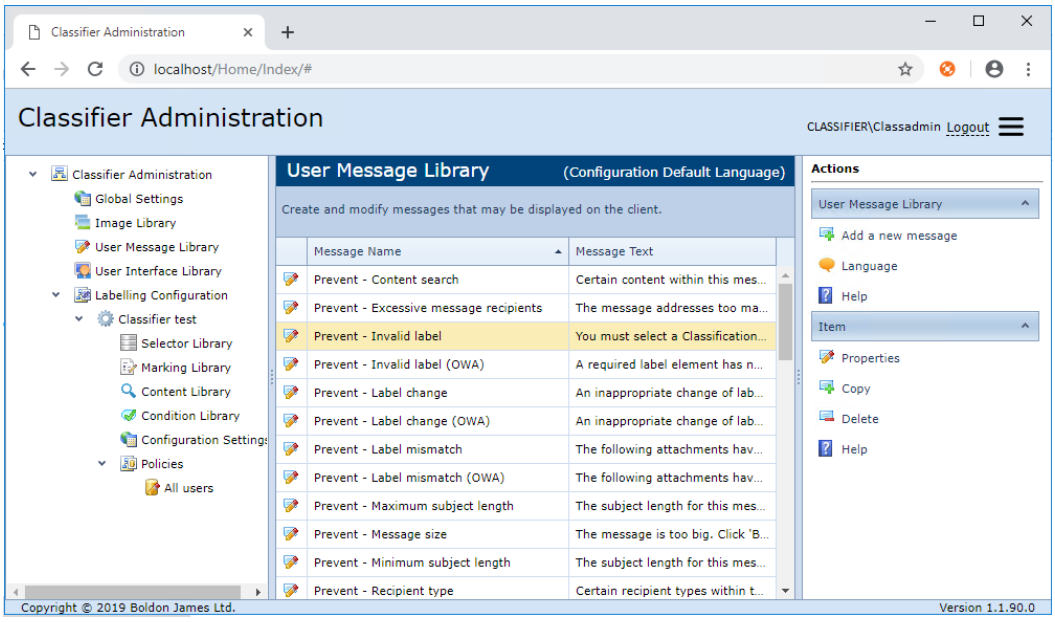


Figure 60: Classification Mandatory – message summary

6.1.2 Define Rule to Perform label validity checks for emails

- ❑ Select **Policies / All users**

- ❑ Choose **Set Rules** Tab and select **Always**
- ❑ Choose **Add a rule** to launch the Rules wizard. Click **Next**.
- ❑ Choose **Outlook emails** and click **Next**.
- ❑ Select **Check rules** from the Filter rule categories drop down
- ❑ Choose **Check these mandatory selectors. Warn ….**

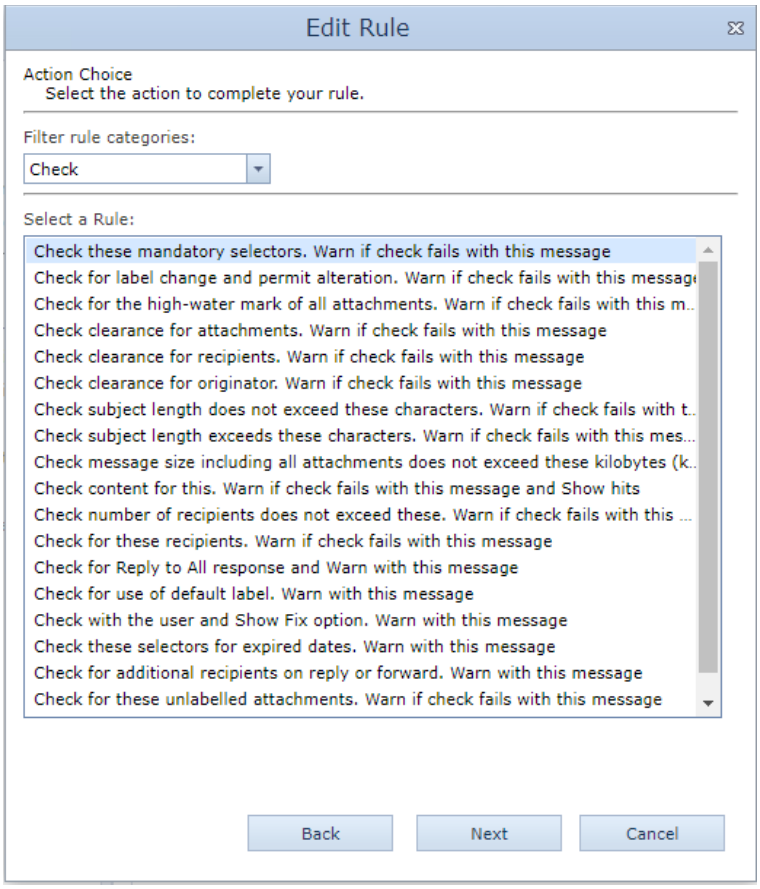


Figure 61: Classification Mandatory rule

- ❑ Click **Next**

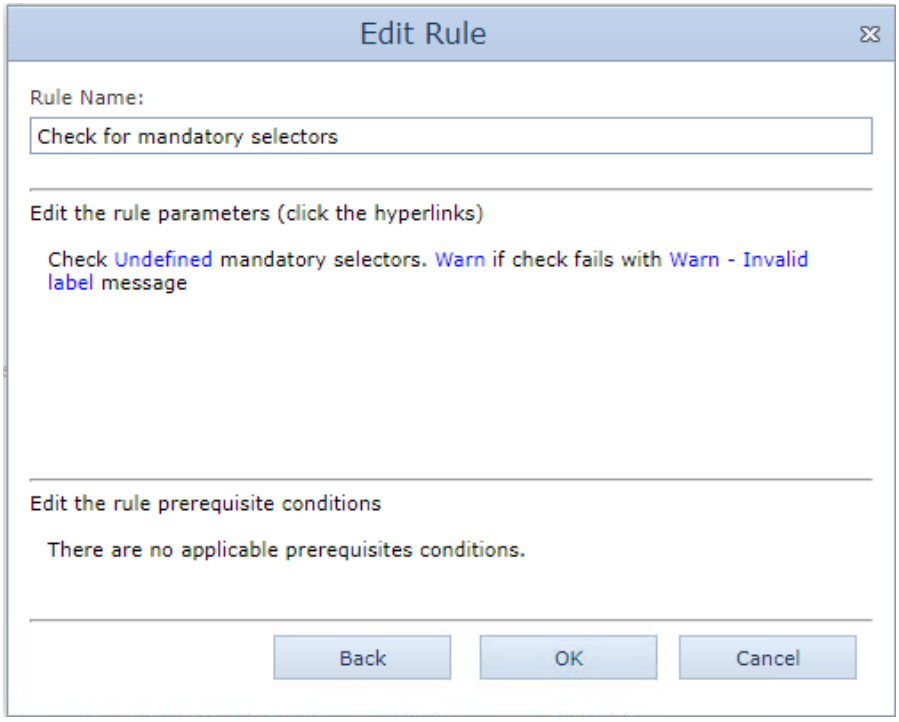


Figure 62: Check for mandatory selectors

- ❑ Click on the hyperlink called **Undefined**.
- ❑ Set Classification to **Mandatory** and Department to **Optional**.

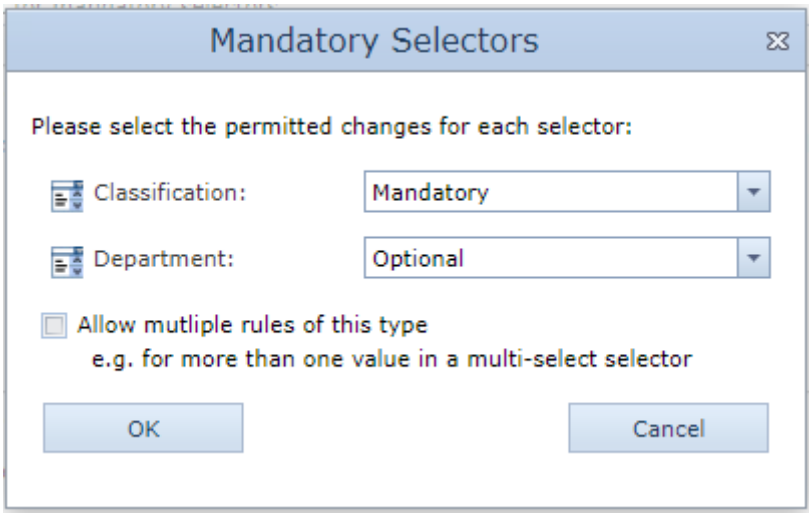


Figure 63: Choose Mandatory selectors

- ❑ Click **OK**.
- ❑ Click on the **Warn** hyperlink and select **Prevent**.

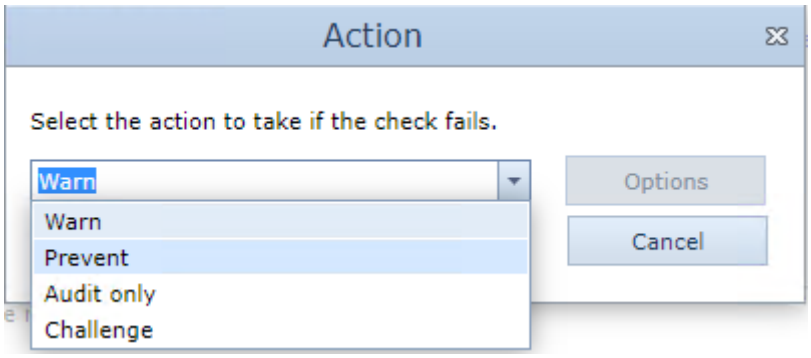


Figure 64: Advise User - Prevent

- ❑ Click **OK**
- ❑ Click on the **Warn – Invalid Label** hyperlink and select **Prevent – Invalid label** from the drop down list. Then click **OK**

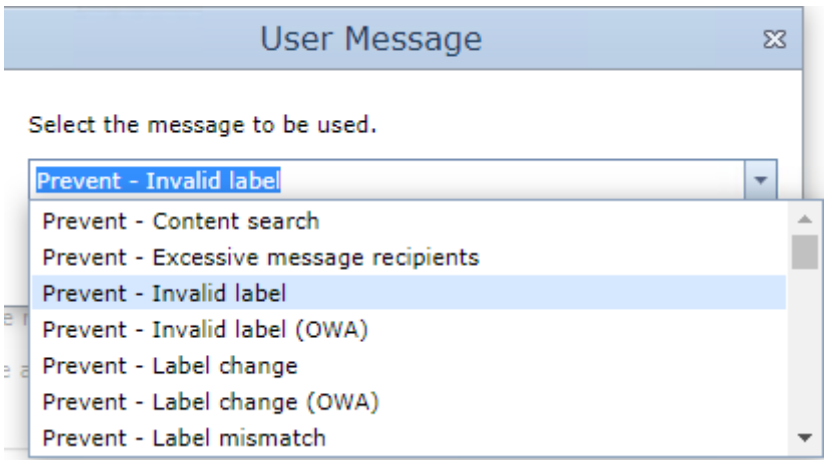


Figure 65: Message for Classification Mandatory rule

- ❑ The rule definition shows the updated settings.

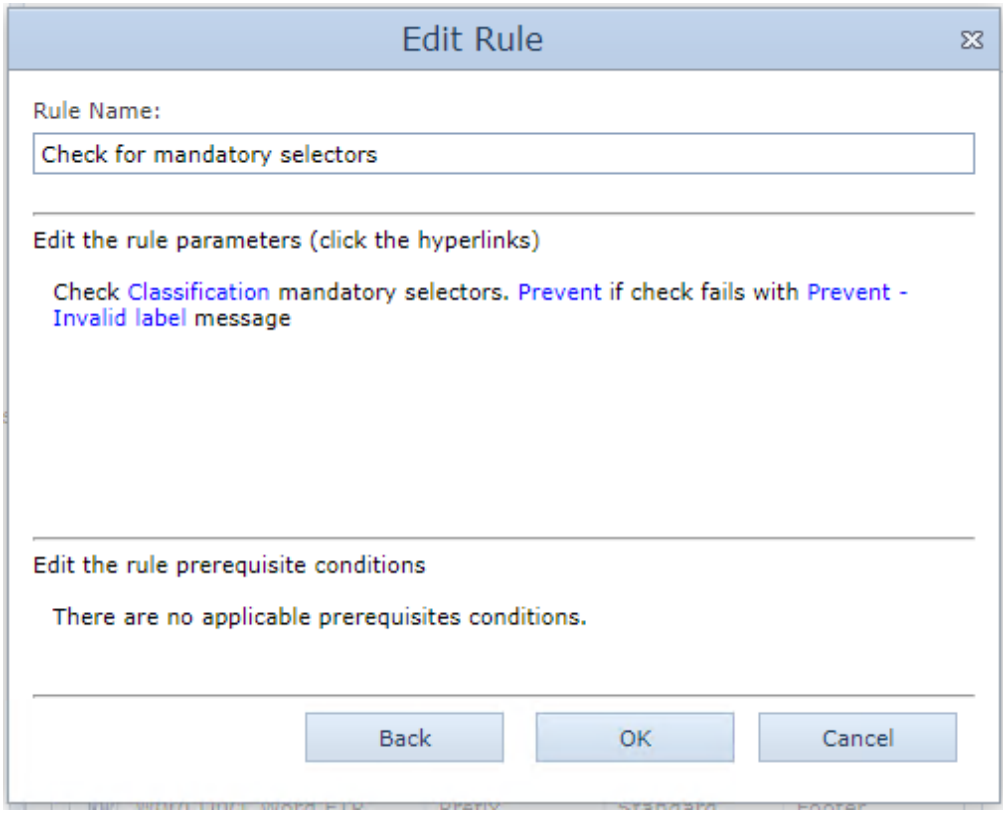


Figure 66: Updated rule definition

- ❑ Set the rule name to **Classification mandatory**
- ❑ Complete the wizard by clicking **OK**

6.1.3 Disable Show the label dialog when mandatory label

The **Prevent – Invalid label** message used will not appear if the **Show the label dialog when mandatory label** option is set.

- ❑ Select **Configuration Settings**.
- ❑ Open **Classifier Application settings**.
- ❑ Select the **Outlook Settings** tab.
- ❑ Disable **Show the label dialog when mandatory label**.

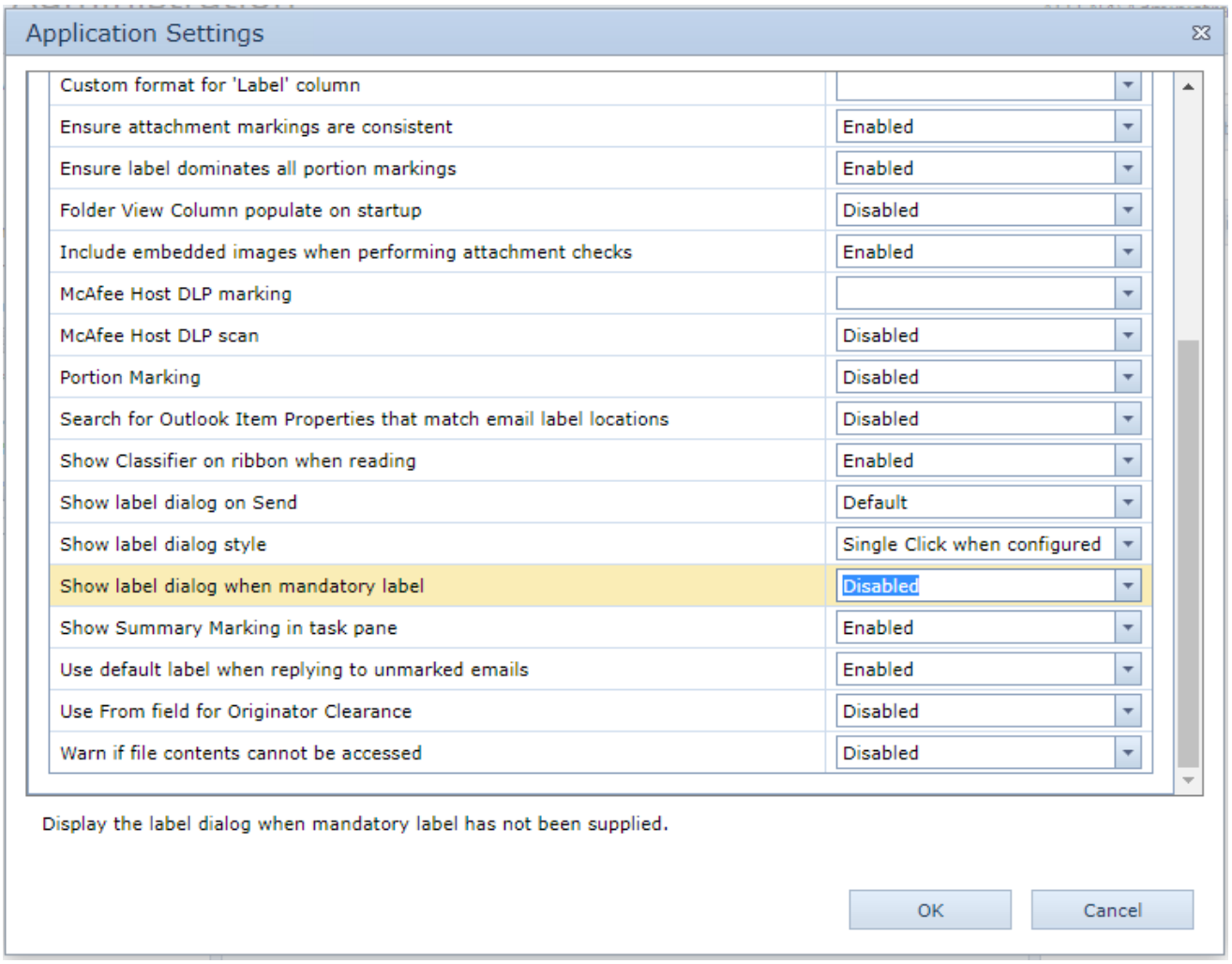


Figure 67: Disable Show the label dialog when mandatory label

6.1.4 Demonstrate the additional features

We must publish the configuration changes and then test the clients to check the effect.

- ❑ Select **Classifier Administration**. Choose **Publish Configuration**. Choose **File Store**. Set the publish reason to **Classification Mandatory** and click OK.
- ❑ Click **OK** on the confirmation dialog.
- ❑ Logon to CT-CL-1 as Salesuser1.
- ❑ Start Outlook and compose a new message setting the Classification to **blank**.
- ❑ Click **Send**. The validity check will trigger and present the following dialog displaying the configured message.

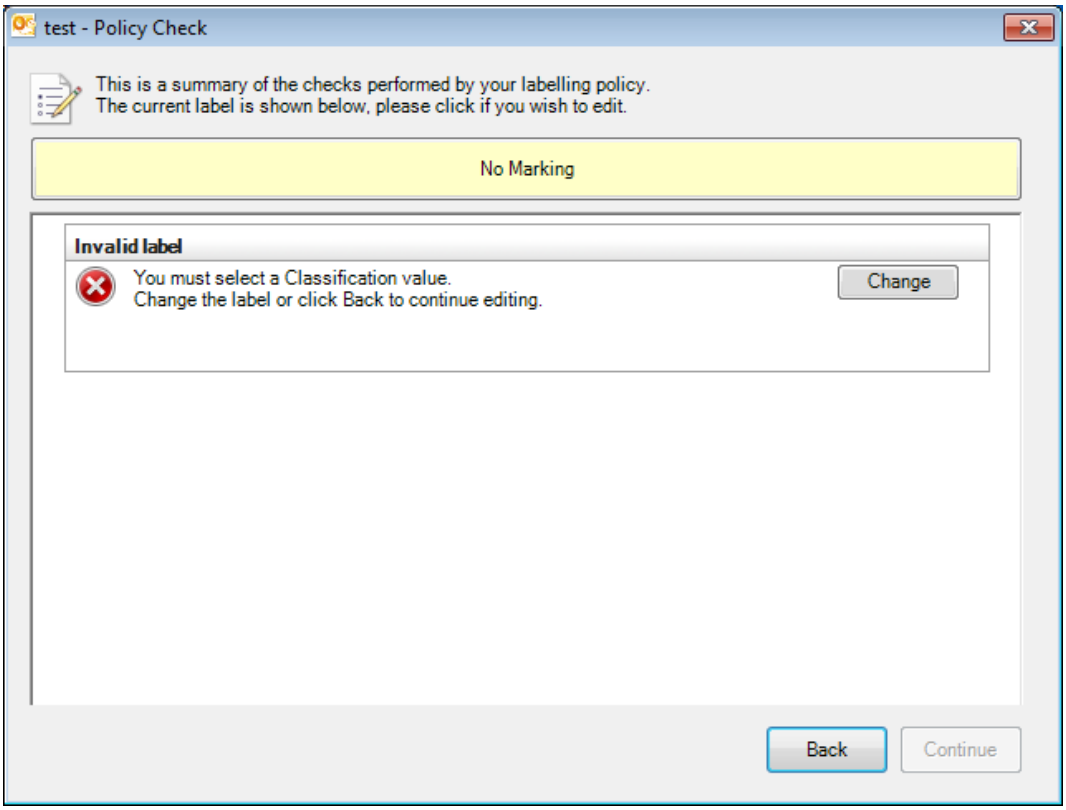


Figure 68:: You must select a Classification

- [The above dialog does not appear if **Show the label dialog when mandatory label** is Enabled].
- Click the **Change** button that will present the following dialog allowing the user to supply a value for Classification.

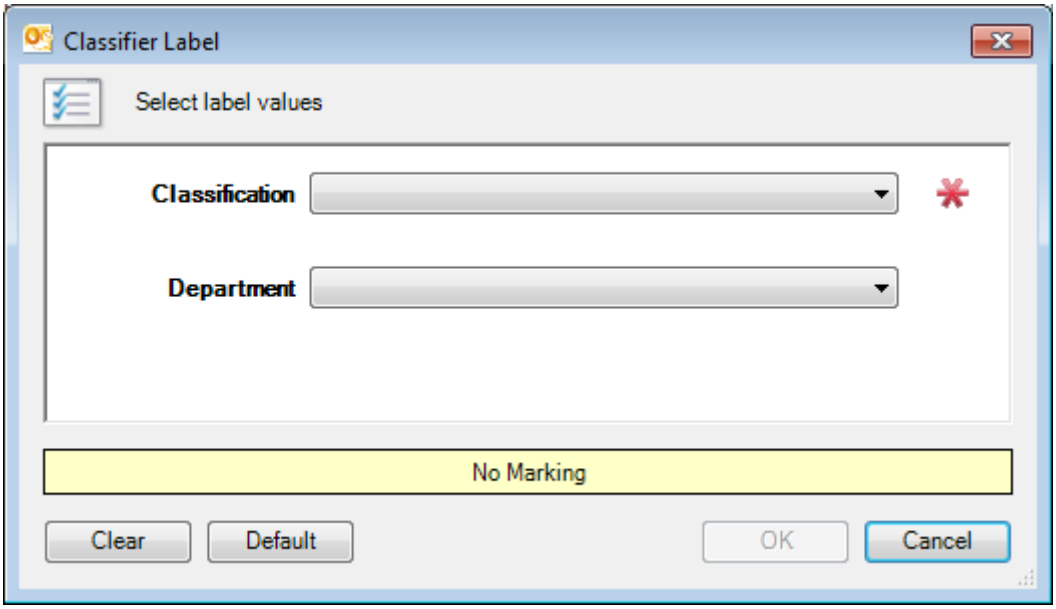


Figure 69: Select a label

- Choose **Public** and click **OK**.
- A Policy resolution dialog will then appear.

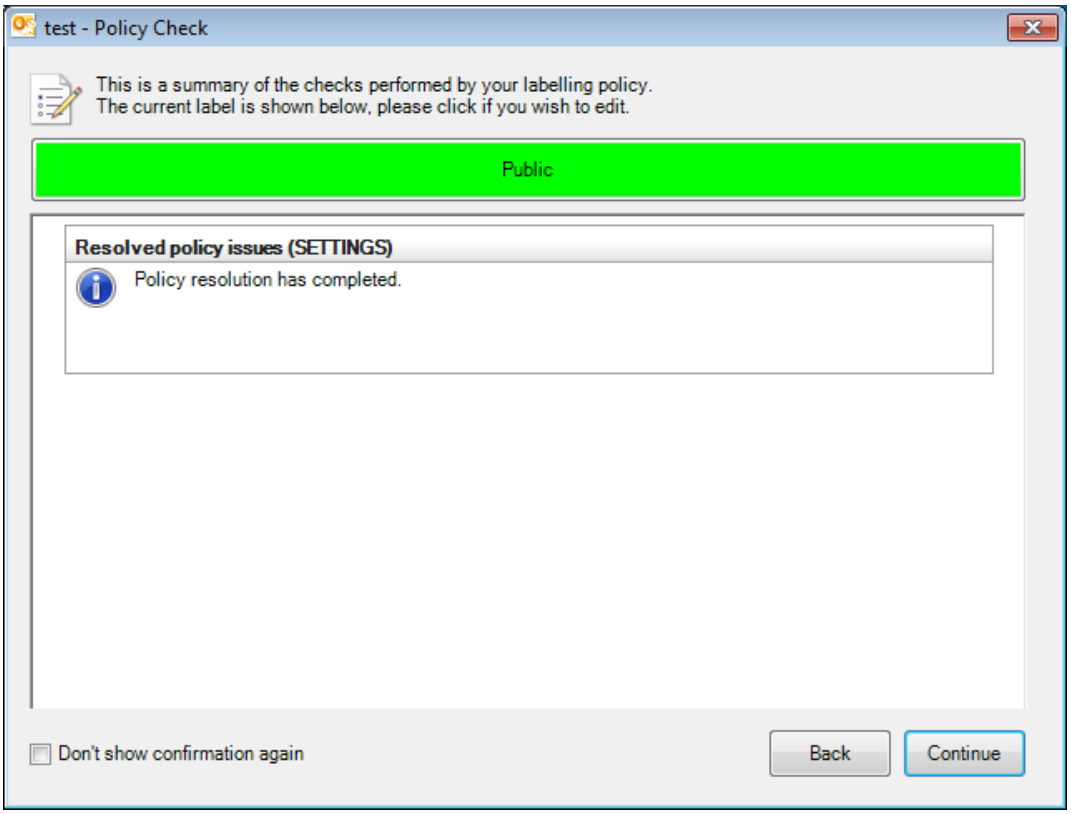


Figure 70: Policy resolution

- [The above dialog does not appear if **Show the label dialog when mandatory label** is Enabled].
- Click **Continue** and message submission will now proceed.

7 EMAIL DOMAIN CLEARANCES

This section shows you how to use Classifier Clearance checking features to limit the label values that external email recipients can receive.

An Email Domain Clearance defines a set of security attributes (label values) and an address space. Addresses that match the address space have permission to receive emails labelled for the designated label values.

The sequence requires the following:

- Ensure Clearance Check Email Domains is enabled
- Configure an Email Domain Clearance for an external domain
- Establish a Rule to perform recipient Clearance Checks when sending emails.
- Locally test the changes
- Publish the configuration changes and test the Client environment

The example creates one new Email Domain Clearance for an email domain called **abc.xyz**. The email domain does not exist, but we can demonstrate the mechanisms to the point of receiving a Non-delivery notification.

7.1 Ensuring Clearance Check Email Domains is enabled

Global Settings/Application Settings/Clearance Check Email Domains has two effects if enabled:

- It directs the Email Classifier to perform Clearance Checks on external recipients when sending an email.
- It controls use of Clearance Settings/Email Domain Clearance within Classifier Administration.

❑ Select **Global Settings** and select **Application Settings**.

❑ Set **Clearance Check Email Domains** to the **Enabled** option.

7.2 Configure an Email Domain Clearance

Using Classifier Administration

❑ Select **Email Domain Clearance** in the left hand pane.

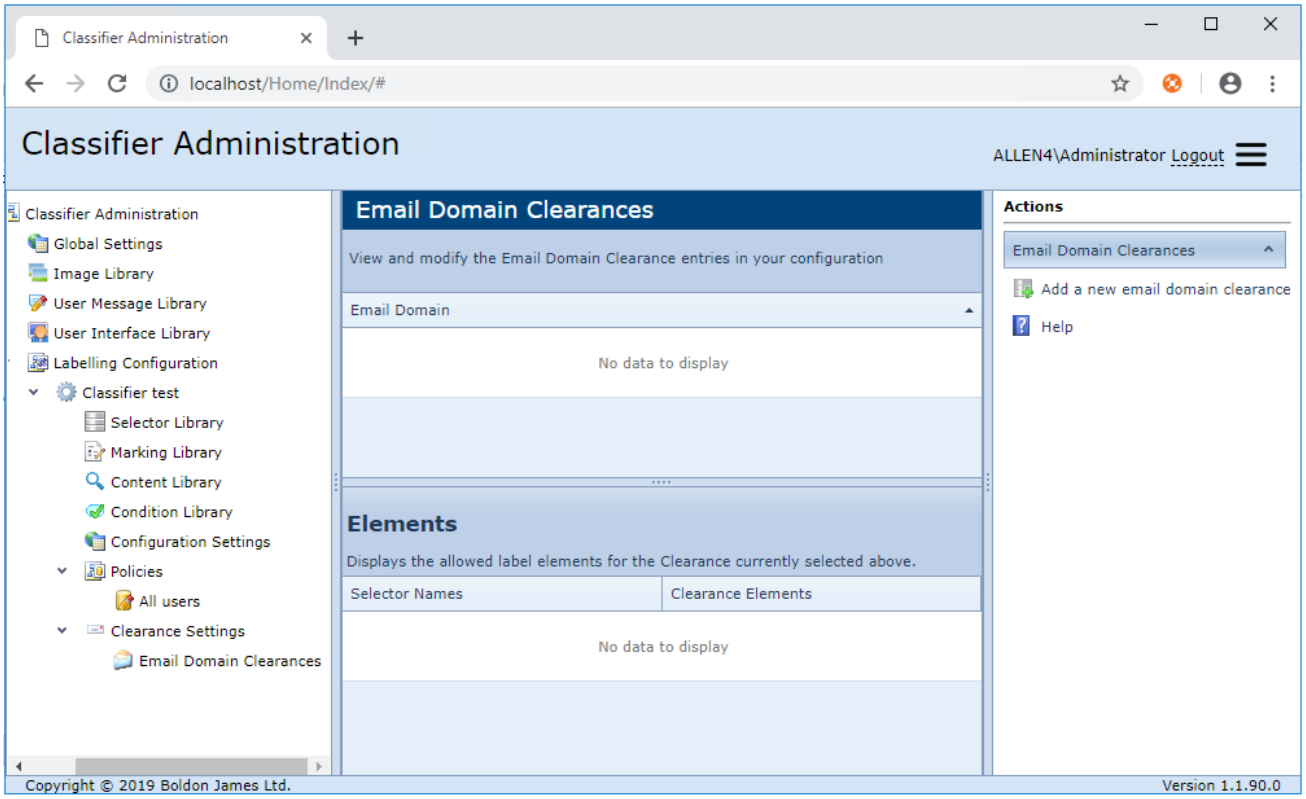


Figure 71: Email Domain Clearance

- ❑ Choose **Add a new email domain clearance**.

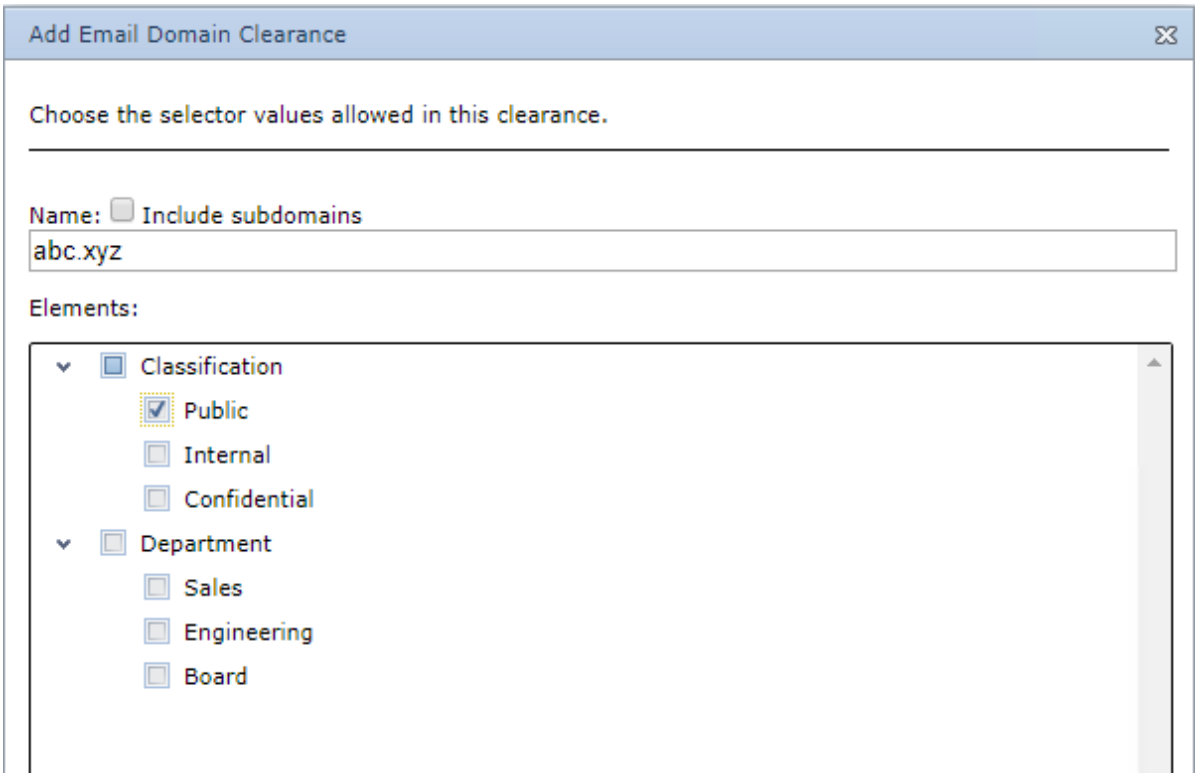


Figure 72: Setting Email Domain Clearance

- ❑ Enter the name of the email domain that you wish to associate a clearance. For example, **abc.xyz**.

- ❑ Select the default clearance for the domain. In this example, we will choose **Classification** / **Public**.
- ❑ Complete the form and the email domain clearance entry will appear as follows:

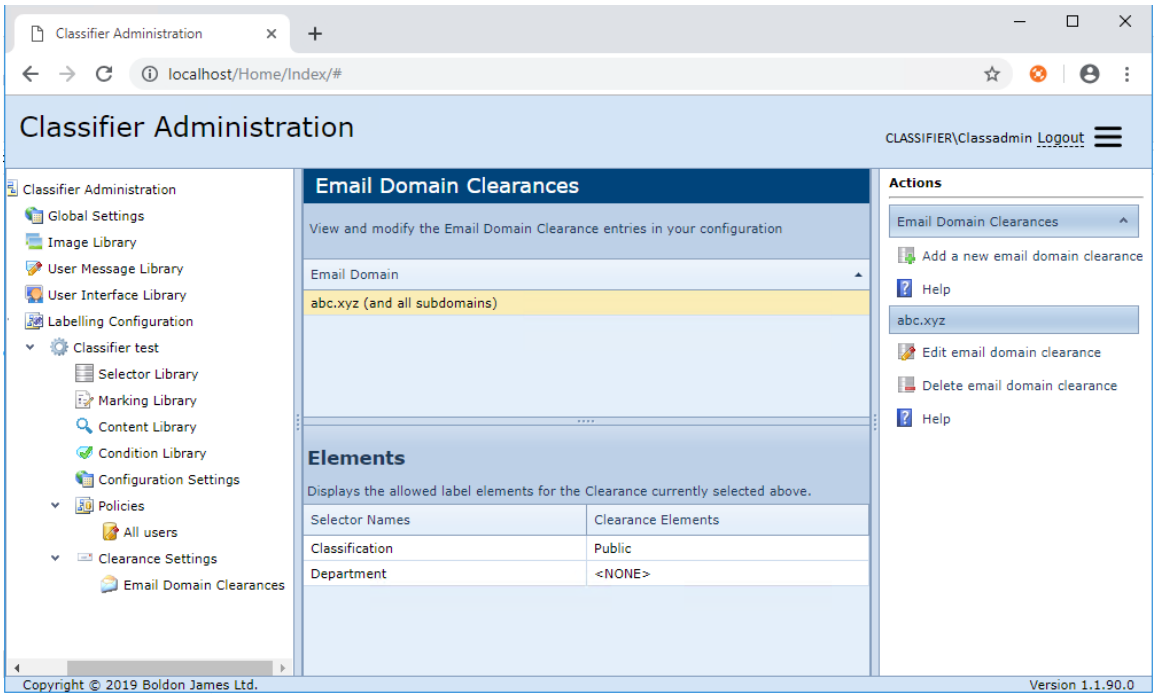


Figure 73: Email Domain Clearance summary

7.3 Establish Rule to perform recipient clearance checks when sending email

7.3.1 Establish a Message for use in the Rule

In this example, we shall use a pre-defined message.

- ❑ Select **User Message Library** and select the **Warn – Unapproved recipients** message. Choose **Properties** to view the default configuration. Click **Cancel**.

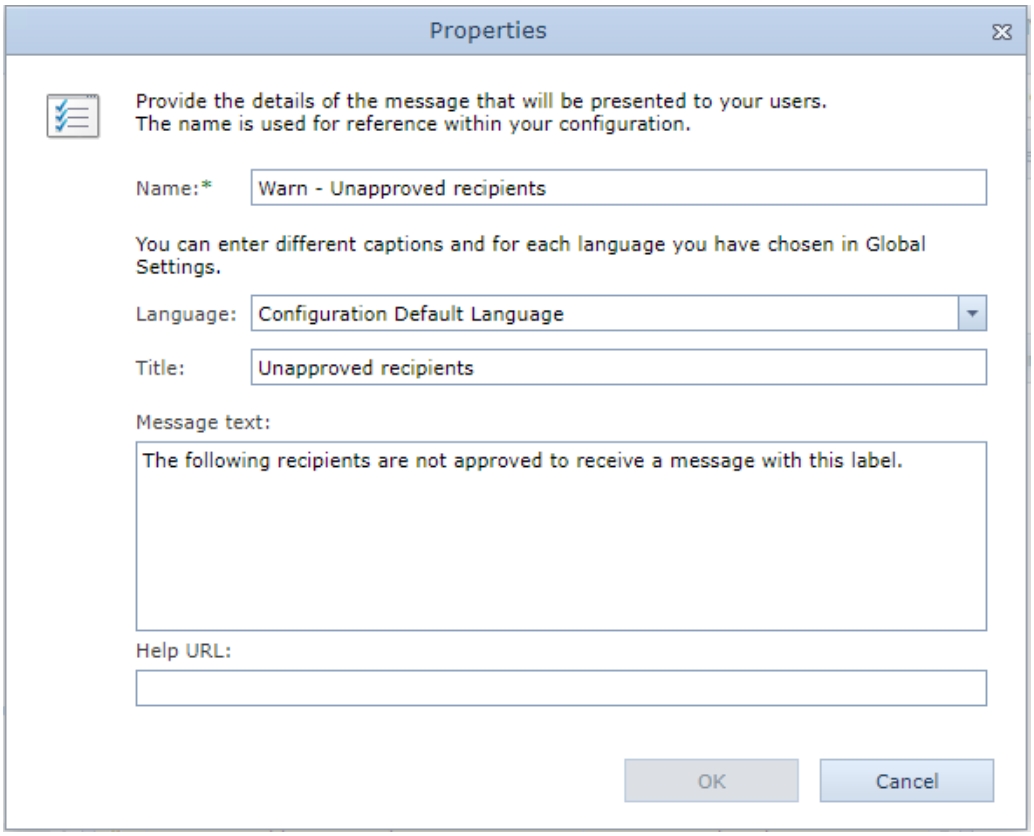


Figure 74: Warn – Unapproved recipients message

7.3.2 Establish Recipient Clearance Check Rule

- ❑ Select **Policies / All users / Set rules**.
- ❑ Select **Always** and choose **Add a rule**.
- ❑ In the Rules Wizard choose **Outlook emails** and choose **Check rules** from the **Filter rule categories** drop down.
- ❑ Select the **Check clearance for recipients…** rule.
- ❑ Leave both the **Warn user** level and the **Warn – Unapproved recipients** placeholder unchanged.

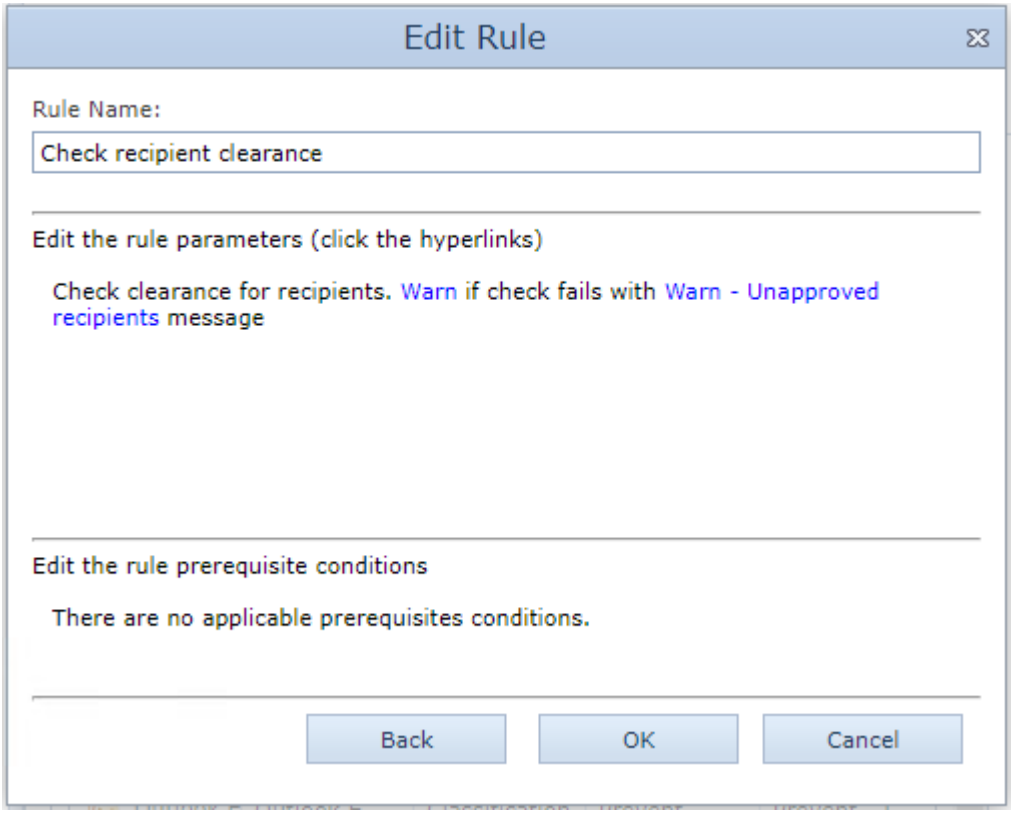


Figure 75: Recipient clearance check rule

- ❑ Leave the rule name unchanged (**Check recipient clearance**).
- ❑ Click **OK** to complete the Rule wizard

7.3.3 Locally test the changes

- ❑ Publish the test configuration by following the steps in section 3.7

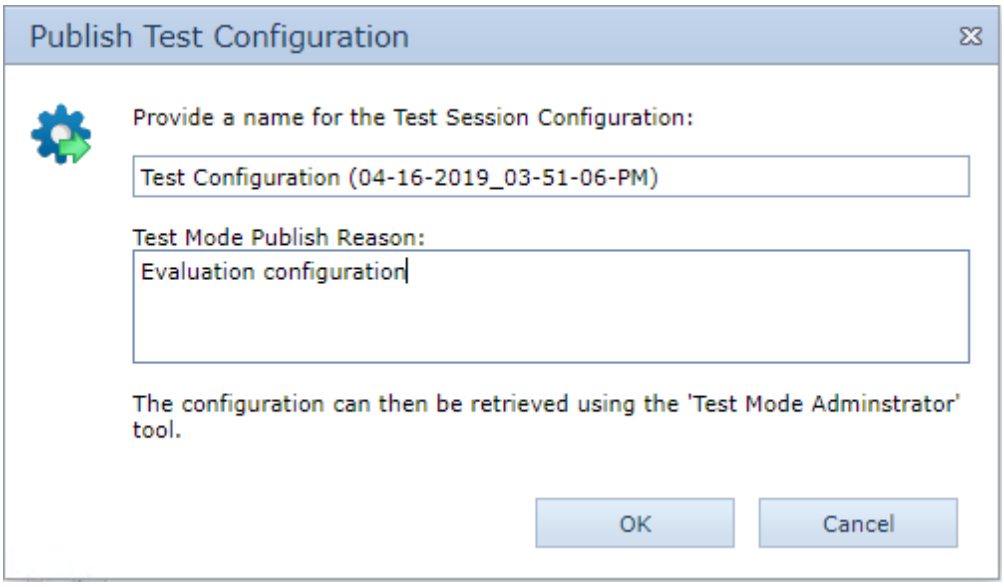


Figure 76: Test the changes

- ❑ Ensure that all Office (Word, Excel, PowerPoint and Outlook) applications are closed.
- ❑ From the Test Mode Administration tool select the appropriate configuration and click **Run Test**. Leave the Test Mode dialog open.

- ❑ Start **Outlook** and **draft a new message** addressed to **another@abc.xyz**.
- ❑ Select **Classification / Internal** and click **Send**.
- ❑ The recipient checks will be performed and a Policy Check dialog will appear:

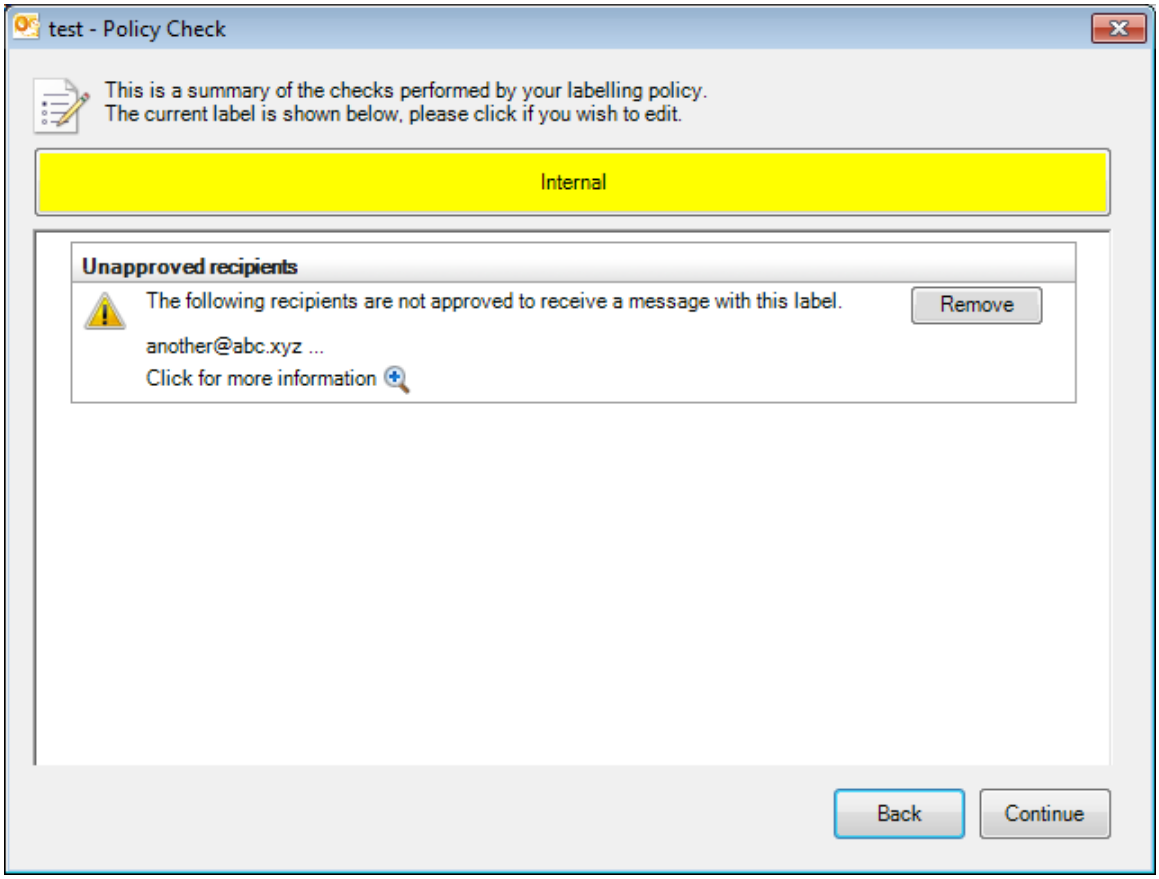


Figure 77 Recipient clearance check effect

- ❑ Click on the **label bar** (showing Internal) and change the Classification to **Public**. Click **OK**.
- ❑ A policy resolution message will appear. Click **Continue** to submit the message.
- ❑ **Close** Outlook.
- ❑ Click **Exit test** on the Test Mode dialog.

7.4 Publish the configuration and test the client environment

- ❑ Select **Classifier Administration**. Choose **Publish Configuration**. Set the Publish Reason to Recipient Check and click **OK** to publish.
- ❑ Acknowledge the confirmation dialog.
- ❑ Logon to CT-CL-1 as SalesUser1.
- ❑ Ensure that all Office (Word, Excel, PowerPoint and Outlook) applications are closed.
- ❑ Start Outlook and draft a new message addressed to **another@abc.xyz.**
- ❑ Select **Classification / Internal** and click the **Send** button to see figure 77. Proceed as in the previous section.

8 ACTIVE DIRECTORY CHANGES

To publish Configuration via Active Directory as described in the subsequent sections requires an update to the Active Directory schema.

8.1 Extend the Active Directory Schema

Note: For Windows Server 2003 environments: In order to extend the schema, the user logged on to CT-SVR-1 should have permission to write to the configuration container and the schema using ADSI Edit. Install the Windows Server 2003 Administration Tools Pack (adminpak.msi) on CT-SVR-1. The schema extension also requires LDIFDE.EXE to be available which may only be available by default on a Domain Controller system.

Note: For Windows Server 2008 run Server Manager and add role “Active Directory Domain Service” then “Active Directory Lightweight Directory Services”.

- From the Classifier **Base Bundle** open the **Classifier Administration Server** folder and then the **Active Directory Schema Extensions** sub-folder. Run **BJ Schema Extension.msi** (or Setup.exe)
- From the Start menu on CT-SVR-1, Run **Classifier Schema Extension** from the **Boldon James** folder.

Note: Extending the schema is a non-reversible operation.

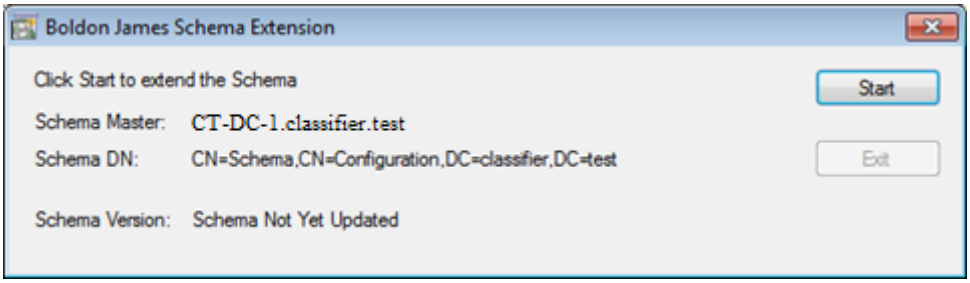


Figure 78 Schema extension

- Click **Start** to update the schema.
- The tool will update the Active Directory schema and show a confirmation dialog - click **OK**. Click **Exit**

9 DEPLOY CONFIGURATION VIA ACTIVE DIRECTORY

After extending the Active Directory schema, it is possible to Publish Classifier Configuration via Active Directory rather than shared file store. Changing from publication via File Store to publication via Active Directory involves two steps:

- Publish the Configuration to Active Directory
- Changes to direct the client to retrieve configuration information from AD rather than a File Store location.

9.1 Publish Configuration to Active Directory

- ❑ We are changing from Publication via File Store to Publication via AD, so we will first retrieve the current master configuration from its File Store location.
- ❑ Logged on to CT-SVR-1 as Administrator, from the start menu run **Boldon James / Classifier Administration Server**.
- ❑ Select **Classifier Administration** and choose **Get Server Configuration**.

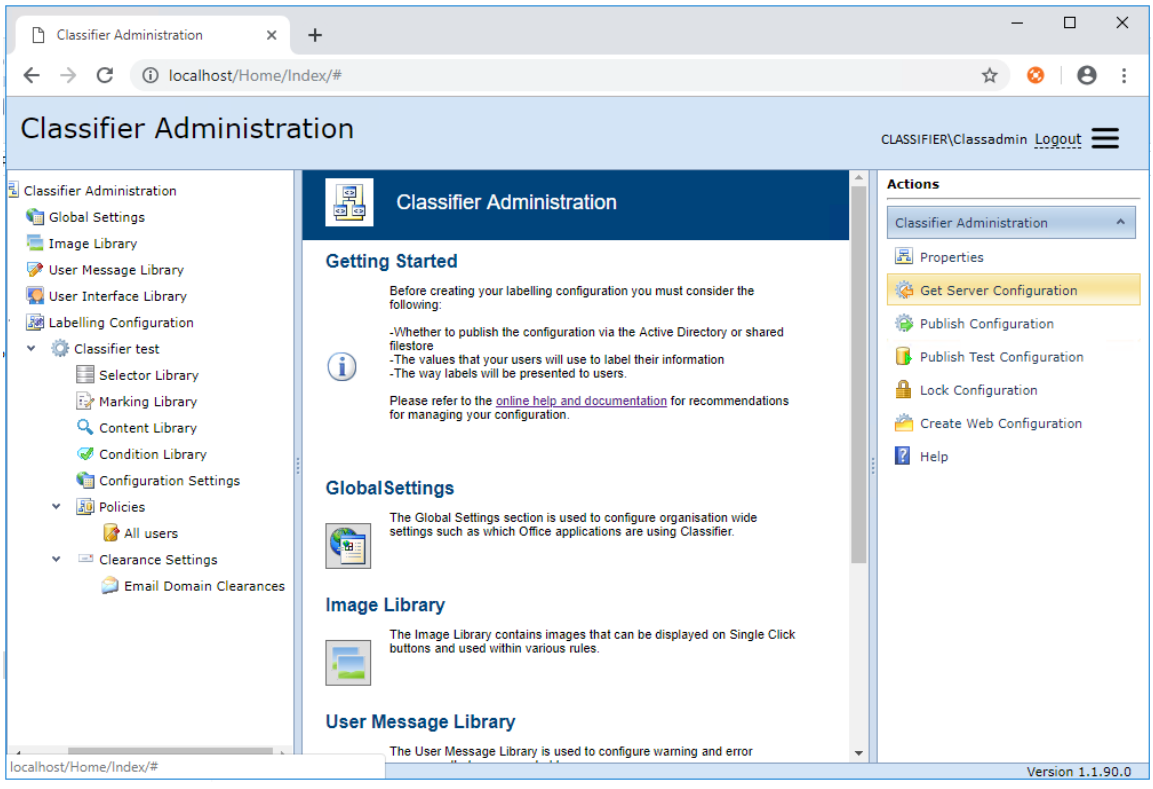


Figure 79: Get Server Configuration

- ❑ Click **Yes** on the confirmation dialog
- ❑ Choose the **File store** location
- ❑ You can now publish the master configuration to Active Directory.
- ❑ From Classifier Administration, select the **Classifier Administration** node and choose **Publish Configuration.**
- ❑ Change the destination from File Store to **Active Directory** as shown below, and enter a reason of "**Publish to AD**".

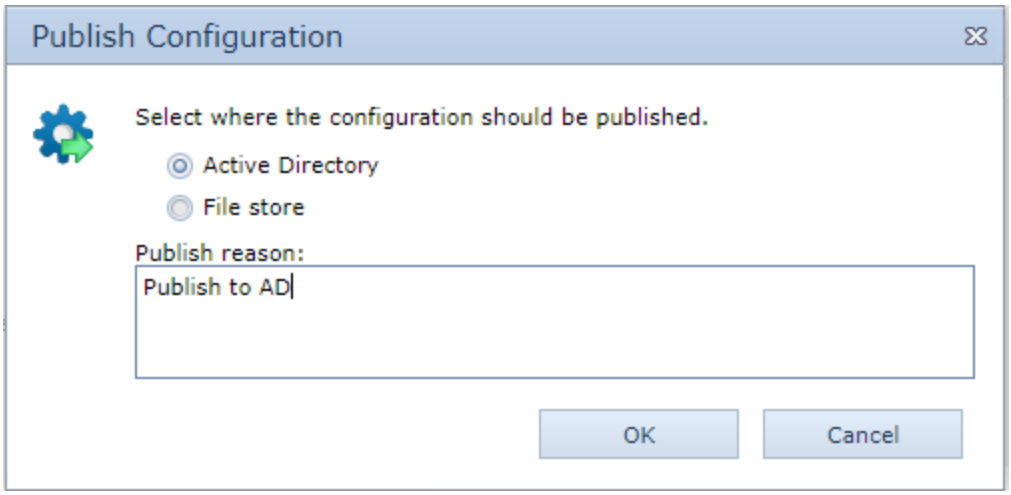


Figure 80: Publish Configuration to Active Directory

- ❑ Click **OK** to complete the action.
- ❑ Click **OK** on the Publish complete confirmation

9.2 Change Registry Settings for Configuration Location

Follow the appropriate sub-section below depending upon whether you are currently setting Registry Keys directly (you followed 4.2.1), or you are using Group Policy (you followed 4.2.2) to set Registry Keys.

9.2.1 Change Registry Directly

- ❑ Change the **ServerRootType** to **1** (This value sets the **Configuration via Active Directory**)
- ❑ Delete the **ServerFileSystemRoot** entry to avoid confusion.

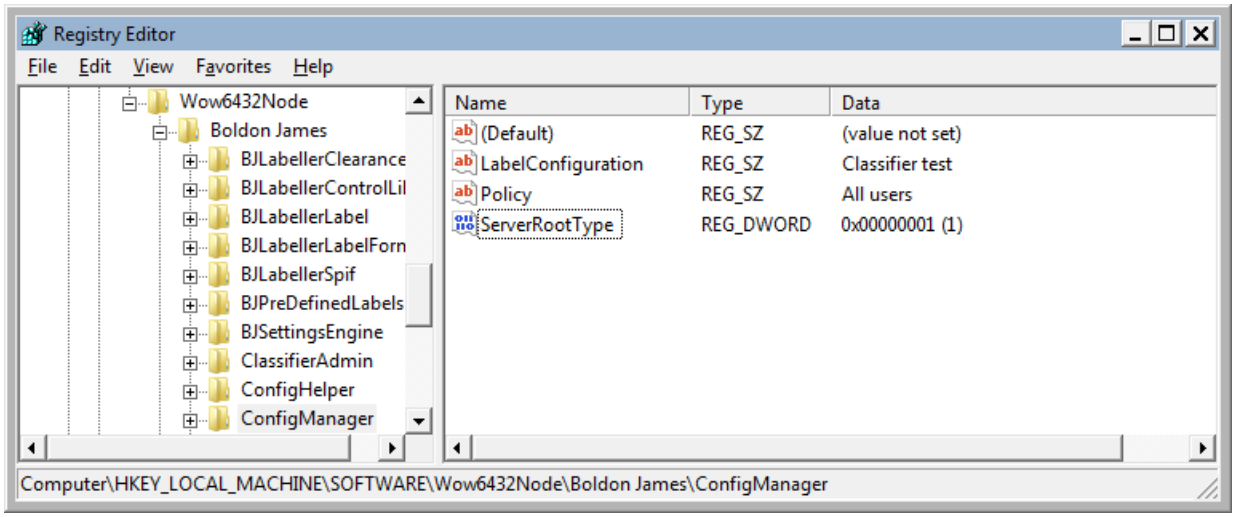


Figure 81: Local Machine Registry Keys

9.2.2 Setting Registry using Group Policy

- ❑ The precise sequence will depend on your environment. The actions below assume that you have already applied the ADM files supplied with the product (see Set the Registry using Group Policy).

- ❑ You can use the Group Policy Management Editor MMC snap-in to get directly to the target tree.
- ❑ Select **Computer Configuration / <Policies> / Administrative Template / Boldon James / Label Configuration** which will present the following settings:

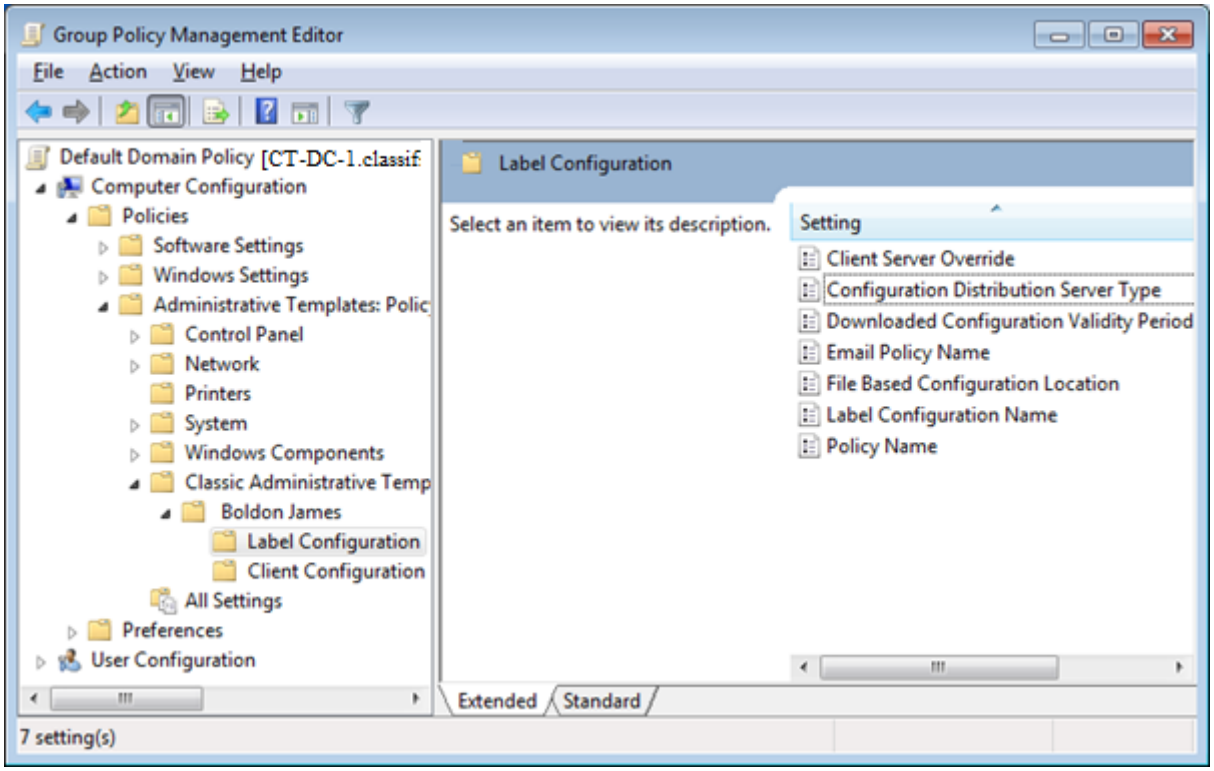


Figure 82: Set Configuration Distribution Server Type

Note: This evaluation scenario does not utilise the Downloaded Configuration Validity Period setting.

- ❑ Select **Configuration Distribution Server Type** and choose Edit **Policy setting** (or **Properties** under 2003).
- ❑ Select **Active Directory** from the drop down and check the **Enabled** option is set. Click **OK**

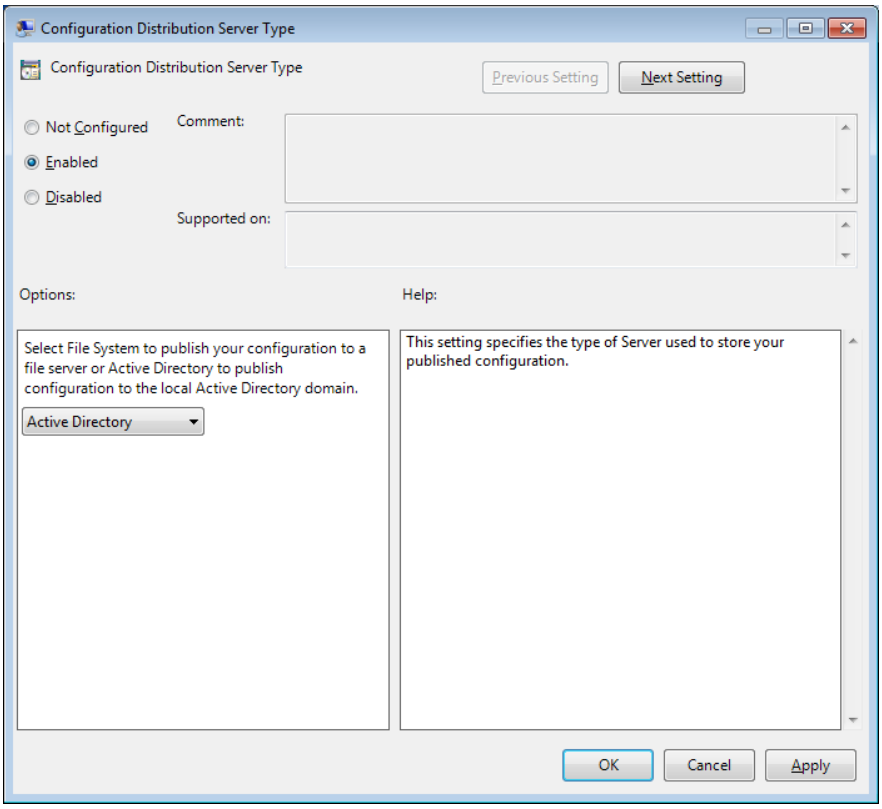


Figure 83: Enable Configuration from Active Directory

- ❑ Select **File Based Configuration Location** and check the **Not Configured** option is set. Click **OK**.

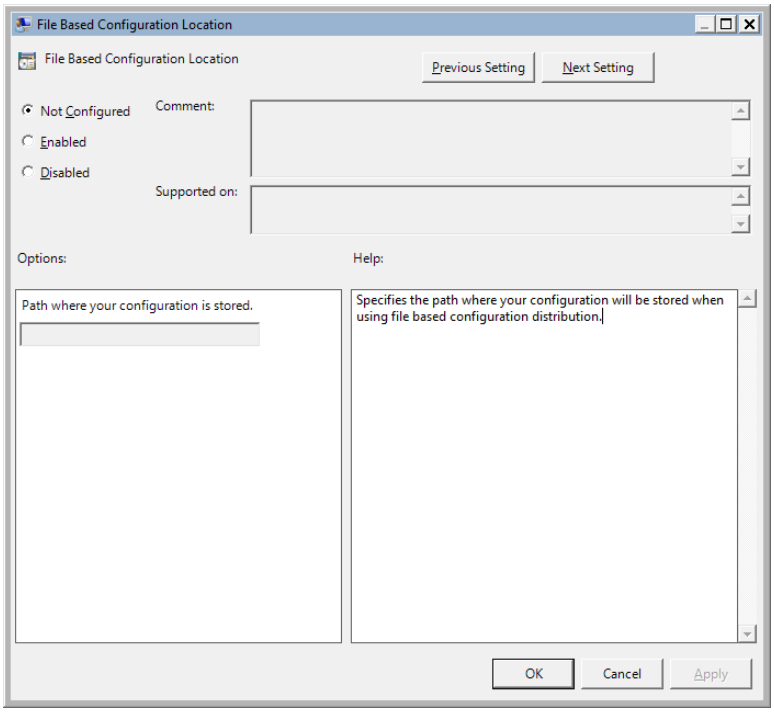


Figure 84: Disable File store location

After a policy update, check the following registry keys have changed on the client:

9.2.2.1 Changed Client Registry Settings

Note: If you are using Group Policy and the relevant keys are not established, then running **GPUPDATE /Force** may be of assistance. In addition, check that the domain recognises the client machine - removing and re-introducing the client can resolve this issue.

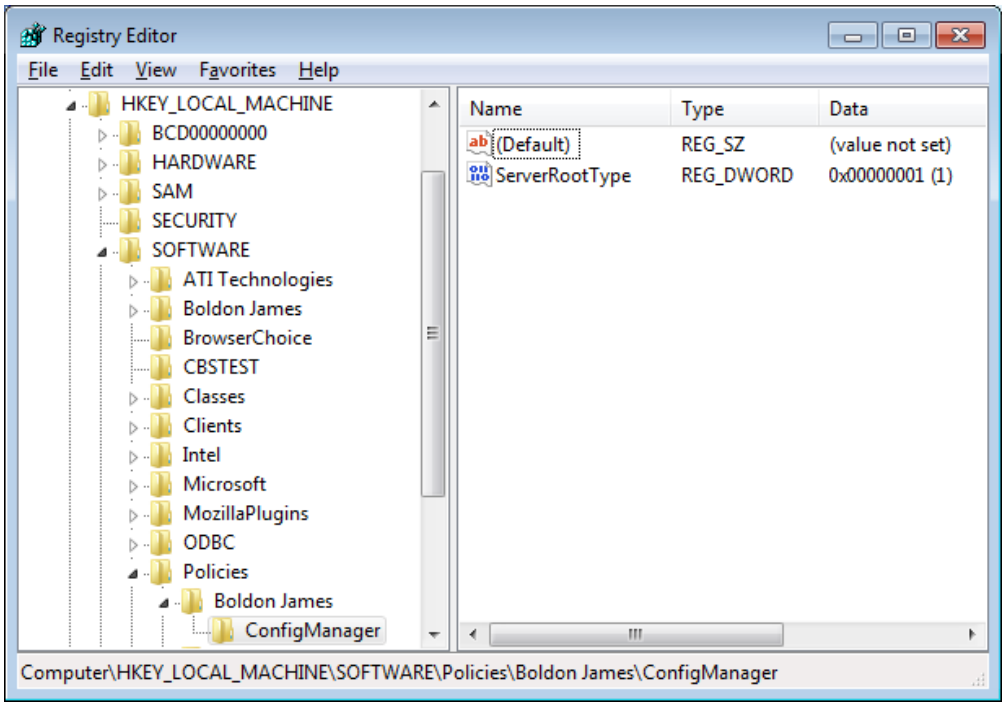


Figure 85: Changed Local Machine Settings