

Classifier Planning Considerations

UM635414

February 19



Gold
Microsoft Partner


© 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.....	3
1.1	Audience.....	3
1.2	Background.....	3
1.3	Classifier Document References	3
2	Planning.....	4
2.1	Labelling	4
2.2	People.....	6
2.3	Control	7
2.4	Orchestration	9
2.5	Infrastructure.....	10
3	Preparation.....	11
3.1	Configuring Classifier to meet my objectives	11
3.1.1	<i>Templates</i>	11
3.1.2	<i>General Configuration</i>	11
3.1.3	<i>Multiple Language support</i>	12
3.1.4	<i>Selectors</i>	12
3.1.5	<i>Marking formats</i>	12
3.1.6	<i>Policy</i>	12
3.1.7	<i>Rules</i>	12
3.1.8	<i>Clearance</i>	12
3.1.9	<i>User Messages</i>	13
3.1.10	<i>Testing</i>	13
3.1.11	<i>Publishing</i>	13
3.2	Creating and maintaining awareness	13
3.2.1	<i>Pre-deployment</i>	13
3.2.2	<i>Post-deployment</i>	14
4	Deployment	15
4.1	Piloting	15
4.1.1	<i>Pilot user community</i>	15
4.2	Knowledge gathering.....	15
4.2.1	<i>Collect user and organisational feedback</i>	15
4.2.2	<i>Collecting and using audit information</i>	15
4.3	Staged introduction.....	15
4.3.1	<i>Education and awareness</i>	15
4.3.2	<i>Community roll-out</i>	16
4.3.3	<i>Increasing control</i>	16

1 INTRODUCTION

1.1 Audience

This document is aimed towards those planning for the deployment of the Classifier client products (Microsoft Outlook, Office and Outlook Web Access). Although other Classifier products (e.g. Exchange Classifier or SharePoint Classifier) are not explicitly mentioned, those products may have bearing on some headings in this document (e.g. should I use labels to control the exchange of information?).

It is recommended that you read the Suite Overview document [2] in order to familiarise yourself with the terms used in this guide.

Note: Throughout this document, Administration Guide means Administration Guide or Administration Server Guide depending upon whether you are using the Administration Console or Administration Server environment.

1.2 Background

This document guides you through a set of steps typically required to create a Classifier deployment. These steps will help you to fulfil your organisation's information classification objectives. This guidance is not exhaustive, but it highlights some important considerations for the deployment.

For further guidance on installation and configuration of Classifier software components please refer to the Starter and Advanced Evaluation Guides.

The guidance provided in this document is divided into three stages:

- 1 **Planning** Understanding what information to gather and the decisions that need to be made before deploying and configuring the Classifier solution. Identifying the aspects of Classifier Administration that are applicable to meeting your objectives (Section 2).
- 2 **Preparation** Converting your information classification objectives and plans into a Classifier Configuration (Section 3).
- 3 **Deployment** How to approach the deployment of Classifier to your target community (Section 4)

1.3 Classifier Document References

Various documents can be found under the Classifier Administration / Classifier Administration Server folder (Base bundle) or via the Start menu after Administration installation.

[1] Administration Guide (UM6351) / Administration Server Guide (UM6440)

[2] Suite Overview (UM6352) / Suite Overview (Server Administration) (UM6455)

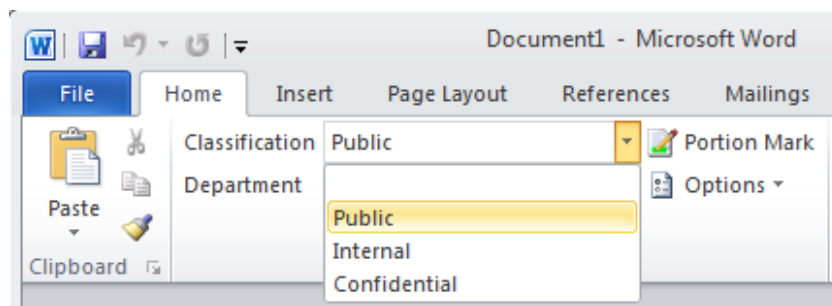
2 PLANNING

This section considers the information you need to gather and what decisions should be made before deploying your Classifier solution.

2.1 Labelling

What will comprise a label?

You will need to decide on the structure of the label that will be used to classify your information. The elements of your label will be presented to your users as labelling choices in the form of Selectors (presented in the user interface of applications such as Microsoft Outlook and Word, Outlook Web Access (OWA) or Lotus Notes – see example Word screenshot below).



In deciding on a label structure, you should consider the following:

- **Do I need to follow any Governmental or Industry standards and guidelines for labelling?**

There may be external guidelines that you need follow (such as the UK Government Protective Marking Scheme, GSC, or the US Controlled Unclassified Information, CUI). However, these may only dictate part of your labelling scheme and there is flexibility for you to choose other labelling elements specific to your needs.

Note: Classifier provides a number of Configuration Templates. These templates contain examples of the elements needed to conform to specific standards and guidelines, such as GSC. You can use one of these templates as a starting point and adapt it to suit your needs (see Administration Guide - Labelling Configurations).

- **What Label Selectors do I need?**

Classifier allows you to establish a label with one or more Selectors. The Values that may be selected by a user are defined by the organisation. Classifier supports the following Selector types: **Single selection list**, and (subject to licence control) **Multiple selection list**, **Text entry**, **Date Picker** and **Date offset list** selectors.

A Selector may represent a hierarchy of values (e.g. to represent a scale of “sensitivity”) or may be more informational (e.g. to indicate a particular project). It is important that the Selectors used and their corresponding values meet the objectives of your business, as well as being meaningful to the users – remember that you will be relying on users to correctly classify information.

Note: You can define all your Selectors in the Selector Library and then use them within a Policy that will be applied to all or part of your user community. If you want to ensure that users always apply a particular Selector then you can configure it to be mandatory. If you want to offer your users a default selection this is also configurable (see Administration Guide - Policies > Policy Label UI > Selector Properties for both of these settings)

➤ **Should I have more than one label structure within my organisation?**

Establishing a common label structure within your organisation is an advantage. However, some communities may have very distinct labelling needs that can only be met, for example, with a distinct Label Selector or specific values of a common Selector. Wherever possible it is advisable to maintain a core label structure that is common to all users and then manage a small number of exceptions.

Note: You can create separate Policies for communities that have differing labelling needs. All the Selectors will still be defined in the Selector Library and you can then apply different sets of Selectors to the separate Policies. You can also identify which Selector values will be used in each individual Policy. (see Administration Guide - Policies > Policy Label UI)

➤ **What do I want to do with my label?**

Once you have decided on the composition of your label(s) you need to determine what information you wish to mark and in what way. Remember that you can mark information assets visually, for example within the header of a Word document, and also mark with metadata, which is hidden marking used by other applications.

➤ **Which assets should I label; that is which of my desktop applications (or OWA Classifier or Notes Classifier) need to be enabled for labelling?**

You should determine which of the following information assets you wish your users to label: Outlook emails; Word documents; Excel spreadsheets; PowerPoint presentations; Project Projects; Visio diagrams; Web emails; Notes emails, CAD files. Depending on the assets you have chosen to label you will need to deploy and enable the Classifier products for the relevant applications. For example, Microsoft Outlook and Word must be enabled in order to label e-mails and documents.

Note: You can control which applications apply labels through the configuration settings (see Administration Guide - Global Settings > Application Settings). Your choice of assets may also be restricted by the Classifier products that you have licensed.

➤ **What visual markings should I apply and to which asset types?**

You can visually mark your assets in different locations and formats to reflect the label applied to the asset. For example, you may choose to apply a First Line of Text (FLOT) marking to emails and a Header marking to your Word documents. The application of markings is achieved through the definition of Rules within a Policy.

Note: Marking Formats and Rules (see Administration Guide – Rules Supported).

➤ **Are there other systems that I wish to control using labels?**

The markings you apply can be used to control other systems that handle the labelled information. This can be achieved using specific visual markings, for example an email

subject line prefix marking of "ENCRYPT:" may be used to trigger the action of a gateway email encryption system.

Alternatively, you can use metadata markings to apply hidden triggers for other systems. For example, an email X-header containing a retention period may be added to direct the actions of an email archiving system. In general, it is preferable to use metadata to control these other systems, as the content is neither visible to users nor directly modifiable.

Note: For Marking Formats, see [Administration Guide - Labelling Configurations > Marking Library](#), and for Rules see [Administration Guide - Policies > Rules Management](#).

2.2 People

Who will be involved in the labelling of information?

You should decide which members of your organisation will need to apply labels and handle labelled information. This may be all of the users in your organisation or a specific community. Having established the relevant labelling configuration and Policy(s) you will have to ensure that users are configured to use the correct policy.

Note: Policies (see [Administration Guide - Configuration Deployment and Client Configuration](#))

Will all the staff involved share a common labelling policy?

If you have identified a common label structure to use across your organisation, then you should only need a single labelling Policy. However, if you want to vary the presentation of any aspect of the labelling interface for particular groupings, or to apply different actions to certain communities, then you will need to consider defining separate Policies for such communities. A user can only operate under a single labelling policy. You should therefore ensure that any groups requiring distinct Labelling Policies do not have overlapping members. Each configured OWA server will apply a single Classifier Policy to all users of that server.

Note: Policies (see [Administration Guide - Configuration Deployment and Client Configuration](#))

Will my users understand labelling terminology?

Whilst the terminology presented to the end users of Classifier is largely neutral, you may wish to adapt this to better meet the needs of your organisation or consider whether you need to present different terminology to particular communities.

Note: User Messages and Selector Library (see [Administration Guide - User Message Library and Labelling Configurations > Selector Library](#))

Will my users need help understanding the labelling policy and their responsibilities?

The user interface of Classifier is simple and intuitive. However, users will still need to understand the principles of your labelling policy and how they are expected to use labels. In addition to any awareness campaign prior to deploying a Classifier solution, you should consider establishing an intranet website describing the principles of labelling and what you expect from your users. The Suite Overview document can be used as the basis for such a website.

Note: The Classifier user interface contains a “help” link that you can configure to direct users to an intranet website containing specific guidance on your labelling policy (see *Administration Guide - [Labelling Configurations > Configuration Settings > General Settings > URL for your labelling help site]*).

Would any users benefit from a quick method of selecting between a set of labels?

Single Click label selection is a **licence-controlled feature** to provide users with quick shortcuts to pre-set labels. This may be of benefit where users will only have a limited number of label choices or where a particular community of users require the simplest possible labelling interface. The Administrator can use the Single Click feature to configure up to twelve separately coloured buttons to appear in the Classifier Label Ribbon Bar, each representing a different label choice.

Note: You can configure Single Click operation on a per policy basis (see *Administration Guide - Policies > Policy Management > Properties > Use Single Click with pre-defined labels*). Single Click is only available under Microsoft Office 2010 or later.

Will users need guiding through the selections needed to choose a label?

Assisted Labelling is a **licence-controlled feature** that can help guide a user through the selections needed to choose a label. For example, if the primary classification of an email is to be “Personal” then the presentation of further business-specific label selectors is unnecessary and can be avoided. The value chosen for one selector can be used to control the values presented for another selector – thus preventing the choice of inappropriate combinations of label values.

Note: You can create Assisted Labelling Policies that provide additional control over the choices presented to the users. You can even define additional selectors as long as no more than 3 are ever presented to the user. (See *Administration Guide - Policies > Policy Label UI > Connect Selectors – Assisted Labelling*)

Will users routinely use only a subset of labels in their work?

The **Favourites** and **Recently used** features are **licence-controlled features** that allow each user to maintain their own set of Favourite labels, and/or allow the system to maintain recently used label values. These features allow users to more easily select the labels that they use most often or that are most significant to their work.

Note: These features are configurable. (see *Administration Guide – Configuration Settings > General Settings > Display of Favourites button* and *Policy Management > Policy Properties > Maximum number of labels to show*)

2.3 Control

Should I focus on creating awareness of asset handling responsibilities?

A significant benefit from an information classification system is that it connects users directly with your information security policy and can serve to remind users of their responsibilities when handling information assets. You should decide to what extent you want your Classifier solution to intervene and inform users of actions that may contravene your security policies, and also to what degree you want Classifier to help educate your users. You may decide to adopt phases of deployment, starting with a focus on creating user awareness, followed by a monitoring of behaviour before finally applying closer control of specific user actions (see also [Staged Introduction](#)).

Note: You can tailor the terminology and textual messages used by Classifier when presenting feedback to your users. Rules can also be used to determine if you wish to warn users of potential policy violations, rather than preventing those actions (see Administration Guide - *User Message Library and Policies > Rules Management*).

Do I need to control what my users can do with labels?

Your classification policy should identify whether the labelling of an asset is essential and to what extent you should restrict the ability of users to change existing labels. You can ensure assets are labelled by mandating the use of some or all of the Selectors of a label. Such a mandate can be flagged in the user interface and also enforced by Rules. Where information assets have already been labelled, you can control whether labels can be changed and if you use hierarchic selectors, whether these can be “downgraded” to a lesser value.

Note: You can apply various supported actions to information by defining Rules. These Rules can be general or only applied if the label matches specific values (see Administration Guide - *Policies > Rules Management*).

Should I check that the content of an email or Word or Excel document is appropriate to the label?

Content Checking is a **licence-controlled feature** that allows you to check that the content of an email (including attachments), and / or Word and Excel documents, contains only content that is appropriate for the label chosen. Where you have important content that can be identified by key words, phrases or regular expressions, then Content Checking rules can be used to ensure that users give such content an appropriate label.

Note: Content Checking rules may be configured on a per-policy basis using the content matching defined in the Content Library. (see Administration Guide – *Labelling Configurations > Content Library*).

Should I use labels to control the exchange of information?

One of the benefits of consistent information classification is that you can control the flow of information by requiring those receiving labelled information to have an appropriate clearance (or privilege) to handle that information. One of the obvious areas to consider for such control is the external organisations with which you exchange information.

Note: You can control the exchange of email with external organisations by setting clearances against e-mail domains (address spaces) and defining Clearance Checking Rules to determine which organisations can receive information bearing specific label values. You can prevent such actions or warn users of potential contraventions (see Administration Guide - *Clearance Settings > Email Domain Clearances*).

Should the control of information exchange extend to internal users?

You may also wish to use labelling and Dynamic Clearances to apply “need to know” principles within your organisation in order to constrain certain information to specific user communities and privileged individuals.

Note: You can assign clearances to individuals or groups of users with User Clearances (see Administration Guide - *Clearance Settings > Dynamic Clearances*).

2.4 Orchestration

Should labelling be used to direct the actions of other systems?

You may wish to invoke the use of other protective technologies based on particular label values. This can also be extended to retention solutions such as e-mail archiving systems. The invocation of some desktop protective technologies is built into Classifier. Other technologies that sit within the flow of information can be controlled by the addition of markings that the target technology can recognise and react to.

Which Protection and Retention systems?

➤ Data Loss Prevention (DLP) and Archiving

Where there are systems that act on email that is “in transit”, for example Email Guards, Gateways and Archiving systems, you may elect to use labels to direct the actions of these systems. In this way you can achieve a finer level of control over these systems. For example, a specific label value can be used to set an archiving retention period.

Note: Rules and Marking Formats (see Administration Guide - Labelling Configurations > Marking Library and Policies > Rules Management).

➤ Digital Rights Management - RMS

If your organisation uses the Microsoft Windows Rights Management Services (RMS) then Classifier has inbuilt support to drive the application of RMS to the desktop. You should consider which assets will need RMS protection and which specific label values will invoke the use of particular RMS templates.

Note: Rules - RMS (see Administration Guide - Office Classifier Features or Email Classifier Features > Policy Rules Application Features > Apply RMS Policy)

➤ Email encryption and digital signature – S/MIME

Where information of a high sensitivity is to pass outside your organisation (or be exchanged within an internal “need to know” group) then you may wish to encrypt and/or digitally sign such emails. Classifier can drive the application of email encryption and digital signature at the desktop by invoking the use of S/MIME security. Having the application of encryption determined by the selection of particular label values removes the need for users to remember when to use encryption. In order to use this facility you will need to ensure that users have suitable digital certificates installed on their systems.

Note: Rules – S/MIME (see Administration Guide - Email Classifier Features > Policy Rules Application Features > Apply S/MIME Security)

Do I need to interact with the labelling schemes of other organisations?

You may receive information from other organisations to which labels have been applied. Such labels, or parts of labels, may be relevant to your organisation and should be mapped into your own labelling scheme. Note you can configure Classifier to look for these label values in specific locations, which may be different to the locations configured in your organisation’s label policy.

Note: Label Locations (see Administration Guide - Labelling Configurations > Configuration Settings > Label Locations)

2.5 Infrastructure

How will I deploy the Classifier software to my users?

You can use automated and silent installation mechanisms to deploy the Classifier Client software to end users. The most common approach is to use the standard Group Policy mechanism (.MSI file).

How will I publish the Classifier configuration to my users?

Your Labelling configuration can be published to users either through Active Directory or using shared File Store. The choice largely depends on your IT infrastructure.

Note: Configuration and Publication (see Administration Guide - Configuration Deployment and Client Configuration)

Should I gather and analyse Classifier activity?

One of the valuable outputs from Classifier is the detailed knowledge of how your users behave in respect of your security policy. This knowledge is generated in the form of Windows Event logs that you can tune to reflect the precise behaviours you wish to monitor. Using standard event aggregation tools, these log entries can be analysed by a wide variety of reporting packages to provide you with feedback on the label-related activities of your users. Such reports can be used for compliance monitoring and provide you with indication of where to focus awareness training.

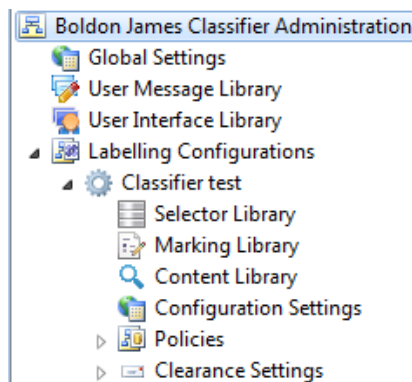
Note: Classifier provides configurable Auditing (see Administration Guide - Settings Applicable across the organisation > Global Settings > Audit Settings)

3 PREPARATION

In preparation for the introduction of your labelling policy, your next step is to develop a Classifier Configuration to implement the policy elements identified in the Planning stage. You should also consider what form of awareness campaign will be needed to help your users understand their responsibilities in classifying information.

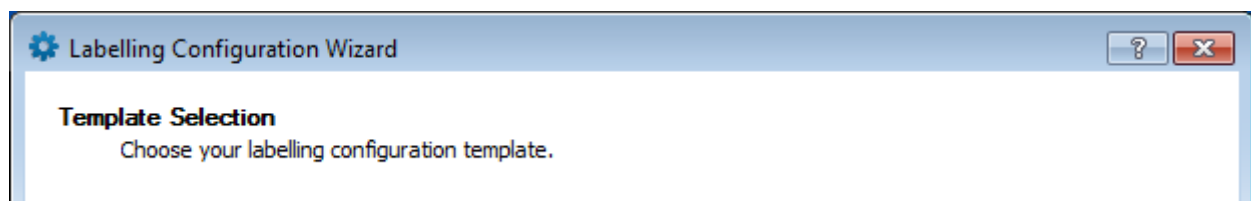
3.1 Configuring Classifier to meet my objectives

In order to produce your Classifier Configuration you will need to install Classifier Administration Console or Classifier Administration Server onto a suitable machine (see Classifier Administration Release Note or Classifier Administration Server Installation Guide for platform requirements). Classifier Administration allows you to map your classification policy into a Classifier Configuration and test that it meets your objectives.



3.1.1 Templates

If at the planning stage, it was identified that an established labelling standard is to be adhered to, then you may decide to start with one of the template configurations offered by Classifier Administration. The configuration can then be tailored according to your requirements. Alternatively, it may be useful to explore a number of template configurations to find one that closely matches your requirements. An 'empty template' is provided if you do not wish to use any of the provided sample templates.



3.1.2 General Configuration

In the planning stage you will have decided which information assets are to be labelled. This decision is applied in Classifier Administration by configuring the individual MS Office applications to be enabled with Classifier.

Note: Global settings and Configuration settings (see Administration Guide –Settings Applicable across the organisation > Global Settings > Application Settings)

3.1.3 Multiple Language support

Classifier uses English as its default language. Classifier allows you to configure the text presented to users to meet your local requirements.

If necessary, Classifier can support multiple languages.

Note: Multiple language support is described under Languages (see Administration Guide – Settings Applicable across the organisation > Global Settings > Languages).

3.1.4 Selectors

The structure of your labels that you identified during the planning phase will be mapped into a set of Selectors configured within the Selector Library of Classifier Administration. This configuration will determine how labelling choices are presented to your end users.

Note: Selector Library (see Administration Guide – Selector Library)

3.1.5 Marking formats

In deciding how labels may be utilised, you will have identified visual labels that can be applied to emails and documents as well as metadata labels that can be embedded in those same assets. Within the Marking Library of Classifier Administration you will configure the individual marking formats to be used when applying these markings. This configuration will determine how markings are presented to your end users and to other systems.

Note: Marking Library (see Administration Guide – Marking Library)

3.1.6 Policy

The configuration of a Policy will bring together the labelling and marking requirements of a particular user community. If you identified groups of users with differing labelling needs then you should configure a policy for each group. Each policy will identify the labelling selectors to present to the users, together with the rules under which markings, checks and other actions are invoked.

Note: Policies (see Administration Guide – Policies)

3.1.7 Rules

The Rules within a Policy control the application of markings, which checks are applied and other operations that may be performed on the assets. Your labelling objectives will commonly be met by a set of rules that apply to all users of a policy, regardless of the choice of label values. However, exceptions to your default rules (based on specific label values) can be configured into a rules decision tree using Classifier Administration.

Note: Rules Management (see Administration Guide – Rules Management)

3.1.8 Clearance

A likely objective of your classification policy is to prevent the exchange of sensitive information with inappropriate parties. This can be achieved by configuring clearance settings for external email domains (i.e. outside organisations). Using this clearance information, you can configure rules to prevent information from passing to the wrong parties, or to warn your users of a potential risk.

Note: Clearance Settings (see Administration Guide – Clearance Settings)

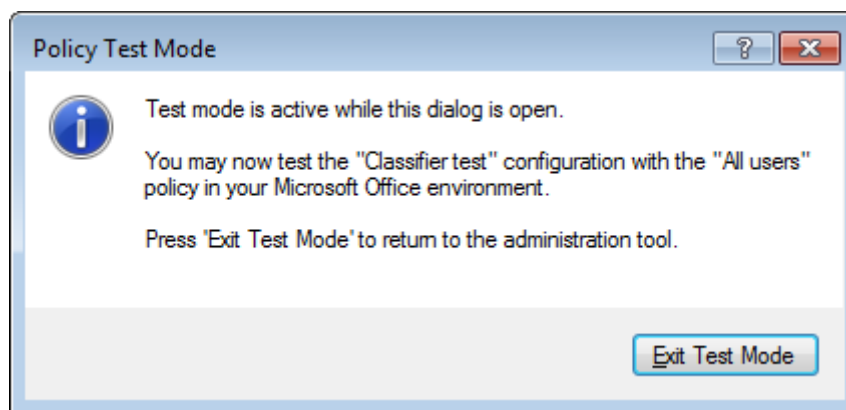
3.1.9 User Messages

If your classification policy requires Classifier to provide feedback to your users on policy contravention, you may wish to tailor the text of the messages presented to your users. This will ensure that the messages contain terminology appropriate to your organisation and to the user's level of understanding.

Note: User Message Library (see Administration Guide – User Message Library)

3.1.10 Testing

In order to check that your Classifier configuration has the desired effects for end users (e.g. that the correct options are presented and markings are applied as you intend), it is advisable to test the configuration 'locally' before deployment.



The Test Mode provided by Classifier Administration and Classifier Administration Server allows you to check the effect of your configuration on the local MS Office applications at any stage in the preparation of the configuration.

Note: Test mode (For Administration Console see Administration Guide - Policies > Policy Management > Run Test Mode). For Administration Server see Administration Guide – Classifier Administration > Publish Test Configuration.

In order to test AD-related operations (i.e. user clearances and publication via AD) you should consider using a full test system (e.g. as described in the Advanced Evaluation Guide).

Note: Test mode only works in a desktop environment. To properly test an OWA Classifier environment you will need a suitable OWA test environment.

3.1.11 Publishing

Once you have completed your Classifier configuration, you can deploy it to the target users by using the Publish Configuration step of Classifier Administration. The outcome of this step will depend on whether you decided to publish the configuration to Active Directory or to a shared File Store.

Note: Publishing and User Deployment (see Administration Guide – Configuration Deployment and Administration Guide – Publish Configuration).

3.2 Creating and maintaining awareness

3.2.1 Pre-deployment

Prior to introducing Classifier to your user community, it is important to provide the end users with the following information:

boldonjames.com

-
- The nature and purpose of your classification policy.
 - What the users will be expected to do.
 - How the users will utilise the Classifier solution.

These elements can take the form of an awareness programme leading up to the introduction of the software itself. This awareness campaign should establish for your users the rationale for consistent labelling of information assets and the role of the Classifier solution in achieving your organisation's objectives.

3.2.2 Post-deployment

Once you have deployed Classifier to your user community, you should consider what form of reinforcement may be needed to the initial awareness campaign and at what intervals. Analysing audit information from Classifier may assist you in identifying which areas of user behaviour may require further education.

4 DEPLOYMENT

In planning your deployment project for Classifier you may wish to consider a phased approach to the introduction and the migration to your full target policy. The following sections outline some possible stages.

4.1 Piloting

4.1.1 Pilot user community

For the initial introduction of Classifier to your organisation, consider establishing a pilot user community and gathering feedback from this group on your classification policy before expanding the deployment to your full target community. If you intend to use multiple Classifier policies tailored to different groups of users, then you could involve a subset of users from each group in this pilot stage in order to gather feedback from a spectrum of users.

4.2 Knowledge gathering

4.2.1 Collect user and organisational feedback

In developing your information classification policy, you will need to liaise closely with those areas of your organisation that will be directly involved in operating the policy. Gathering direct feedback from pilot users or sampling your initial user community will provide valuable guidance on any adjustments to your policy or the Classifier implementation.

4.2.2 Collecting and using audit information

As well as gathering direct feedback from your user community, you should consider using the Classifier audit data to provide objective information on user behaviour and to compare this with the other user feedback.

4.3 Staged introduction

4.3.1 Education and awareness

Prior to introducing Classifier to your user community it is important to provide information to your users on the nature and purpose of your classification policy. The role of an awareness programme was outlined in section 3 Preparation.

Classifier can act as a source of online help for your users in the form of:

- A link to an intranet site describing your classification policy and the use of Classifier
- Individual links to intranet pages that each describe a feedback User Message that Classifier can display to your users when specific policy events occur

This intranet resource can be developed as part of your awareness programme prior to the Classifier roll-out and then form an ongoing reference resource for users.

Note: (see Administration Guide – Labelling Configurations / Configuration Settings / General Settings / URL for your labelling *Help site and User Message Library / Add a New Message*)

4.3.2 Community roll-out

You will have had the chance to refine your classification policy and the Classifier configuration based on feedback and monitoring of your pilot community. In addition, your awareness programme will have prepared users for the roll-out of the Classifier solution. The roll-out to your full target community can be conducted in whatever manner best suits your organisation e.g. as a mass deployment or staged in waves.

If a lengthy roll-out period is expected, you should anticipate the effects from the transitional situation where some users may be equipped with Classifier and others are not. The exchange of emails between such users will continue to propagate the use of unlabelled information and so you should prepare your users for this transition to avoid unnecessary support queries.

4.3.3 Increasing control

The objective of your classification policy may be to apply restrictions on certain user activities; however you may choose to adopt a phased approach towards applying such controls by migrating your Classifier configuration between the following stages:

- starting with establishing user awareness, introducing labelling to the organisation and monitoring user behaviour (e.g. focussing Classifier rules on audit-only actions and providing online help to users).
- moving to providing direct warning feedback to users on policy contraventions (e.g. migrating rules from audit-only actions to applying warning actions, and/or making Selectors mandatory).
- finally adopting preventative controls (e.g. migrating rules from warning actions to applying preventative measures).