

CA DataMinder

Policy Guide

Release 14.6



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA DataMinder™

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- [Enable Regionalized Policy Engine Lookup](#) (see page 299)—How to apply different policy depending on the Policy engine's region.
- [<Who> - Data Lookup Commands](#) (see page 314)—Sent-on-Behalf-of users are now detected as Senders by default.

Contents

Chapter 1: What Is Policy? 15

Introduction	16
Who-When-What	17
Who.....	17
When.....	17
What.....	19

Chapter 2: What Is in a User Policy? 21

Summary	21
Triggers.....	21
Email triggers	22
Data In Motion Triggers	22
Data At Rest Triggers.....	23
Application Monitor Triggers	23
Actions.....	24
Email Actions.....	25
Data In Motion Actions	26
Data At Rest Actions.....	27
Application Monitor Actions	28
Control Action Precedence	29
System Settings	30
Document Classifications	30
Definitions.....	31
User Notifications.....	31
Other System Settings.....	31
Extensions	32

Chapter 3: Whose Policy Is Applied? 33

Email Activity.....	33
File Monitoring and Scanning.....	34
Printed Documents	35
Web Activity	35
Application Monitoring	36
Internal and External Email Addresses.....	36
Identifying Internal and External Senders.....	36
Exempting Internal Emails From Policy.....	37

Flagging Emails As Internal.....	38
Exempt Users	38
Manually Exempt Users From Policy.....	39

Chapter 4: How Policy Works 41

Policy Processing	41
Applying Triggers to Emails	43
Applying Triggers to Files	43
Applying Triggers to Web Events	43
Applying Triggers to IM Conversations	44
Optimized Policy Processing	44
Policy Inheritance	45
Parent-Child Policy Inheritance	45
Policy Branch Inheritance	46
Policy Version Numbers	47
Policy Version Example	47
Reported and Assigned Policy Versions	49
Policy Folders and Settings.....	49
Disabled Policy Folders.....	50
Enforced Policy Folders and Settings	51
Hidden Policy Folders and Settings	53
Controlling Policy Changes	55

Chapter 5: Editing Policies in the Administration Console 57

User Policy Editor	57
Edit a Policy	58
Find a Policy Folder or Setting	59
Policy Reports.....	60
Generate Policy Reports	61
User Definitions.....	62
Export, Import, and Copy Policies	63
Included, Excluded, and Ignored Items	64
Define a Policy List	67
Wildcards and Policy List Items	68
Combination List Checking	71
Multiple Message List Items	71
Copy and Import List Items	73
Changing the List Source	76

Chapter 6: Editing Policies in the iConsole

77

Available Policies	77
Corporate and Regulatory Compliance Policies	78
Customer / Supplier Treatment Policies	80
Employee Behavior Policies	81
Intellectual Property (IP) Policies	82
Legal Policies	83
Non-Public Information (NPI) Policies	84
Personal Health Information (PHI) Policies	86
Personally Identifiable Information (PII) Policies	86
Security General / Corporate Policies	90
User Defined Policies	93
Available Actions	94
Available Actions: Email	94
Available Actions: Files In Motion	96
Available Actions: Data At Rest	97
Who Do the Standard Policies Apply To?	98
FPP User Groups Created Automatically on the CMS	98
User Accounts in FPP Custom Group	99
Editing Policy in the iConsole	100
Define the Global Options	101
Enable Policy Triggers	102
Edit the Policy Settings	103
Choose a Policy Action	104
Save the Policy Changes	104
Policy Tuning	105
Basic Rules	105
Matching Numbers	106
Ignore Key Words When They Occur in Disclaimers	107
Words That Indicate a Definite Non-Match	108
Positive Indicators	109
Threshold Values	109

Chapter 7: Exempting Users From Policy

111

Exempt Users	111
Manually Exempt Users From Policy	112

Chapter 8: Intervention Setting

113

Supported Intervention Options by Client	113
Supported Intervention Options: Email Server Agents	114

Intervention Setting: Advise Encryption	116
Intervention Setting: Block with Notification	117
Intervention Option: Block Quietly	118
Intervention Option: Block (File Events)	119
Intervention Option: Categorize - Single Category Only	119
Intervention Option: Categorize - Multiple Categories Allowed	120
Intervention Option: Categorize	120
Intervention Option: Delete (Scanned Files)	121
Intervention Option: DoD Overwrite and Delete	121
Intervention Option: DoD Overwrite and Replace	122
Intervention Setting: Enforce Encryption	123
Intervention Option: Inform	124
Intervention Option: No Further Actions	125
Intervention Option: None	125
Intervention Option: Notify	126
Intervention Option: Quarantine Quietly	127
Intervention Option: Quarantine with Notification	128
Intervention Option: Replace	129
Intervention Option: Warn	129
Intervention Option: Warn (Personal)	130

Chapter 9: Detecting Key Text **133**

Basic Rules	134
Wildcards and Policy List Items	135
Special Characters	137
Hyphenated Words	138
Far Eastern Characters	138
Which Files Can be Searched For Key Text?	139
Which Triggers?	140
Searching Zip Files for Key Text	140
Nested Zip Files	141
Maximum Size for Decompressed Zip Files	141
Searching Embedded Emails for Key Text	142
Search Text Variables	142
Setting a File Size Limit	143

Chapter 10: Protecting Emails **145**

Overview	146

Chapter 11: Detecting Email Addresses **149**

Email Address Matching.....	149
Webmails Detected by the NBA.....	153
Emails Encrypted with Voltage SecureMail.....	154
Forwarding Emails.....	154
Sending Forwarded Emails to Someone Else	155
Account Requirements for Forwarded E-mails	156
Forwarding E-mails to Multiple Addresses	157
Replies to Incoming E-mails	157
Identifying which E-mail Triggered an Automatic Reply	158
Modifying Recipient Fields	159
Integration With E-mail Servers	159
Server-side versus Client-side	160
Intervention Options and E-mail Server Agents.....	161
Automatic Notifications	162
Interactive Warnings	163
Disable E-mail Integration for Specific Sources.....	165
E-mails in Public Folders are excluded from Policy	166
Viruses and Captured E-mails.....	166

Chapter 12: Encrypting Emails **167**

Specify the Encryption Providers	167
X-header Requirements	168
Define Rule for Voltage SecureMail Gateway	170
X-header Limitation in Exchange 2003.....	170
Set Up Encrypt Control Actions	171

Chapter 13: Protecting Files Being Copied **173**

How Does CA DataMinder Protect Files on Removable Devices?.....	173
CFSA Flow Chart: Removable Devices, CD Drives, Network Folders.....	176
How Does CA DataMinder Protect Files in Network Folders?	178
Local Drives Listed As Network Drives Over RDC	180
How Does CA DataMinder Stop Users Burning Files to CD?	181
How Does the CFSA Protect Files in Sync Folders?	182
Applying Policy to Files Being Copied.....	185
Configure the Local Machine Policy	186
Configure the User Policy.....	193

Chapter 14: Encrypting Files Being Copied	201
Overview	201
Specify Which Removable Devices To Monitor	202
Exempt PGP® Portable Devices	203
Configure Encrypt Actions in the User Policy	204
Educate Your Users About the Encryption Utility	205
CA DataMinder Cannot Encrypt Files Copied to Network Locations	207
 Chapter 15: Detecting Fingerprinted Files	 209
About Content Registration (Fingerprinting)	210
Fingerprinting Components	210
Set Up Triggers to Detect Fingerprinted Files	212
Search for Fingerprinted Documents	213
 Chapter 16: Controlling What Users Can Print	 215
Overview	215
When Do Triggers Activate?	216
CPSA Flow Chart	217
Apply Policy Triggers to Printed Files	219
Specifying Printer Names	219
Do Not Specify File Names	220
Disable Print Screen Button	221
What Data is Captured?	222
 Chapter 17: Stopping Data Leaks to the Cloud	 222
About the Client Network Agent	223
How Does CA DataMinder Stop Data Leaking To the Cloud?	225
Applying Policy to HTTP Activity	226
Configure the Local Machine Policy	227
Configure the User Policy	228
 Chapter 18: Protecting Data at the Network Boundary	 231
Files Entering or Leaving the Corporate Network	232
Local Drives Listed As Network Drives Over RDC	233
Detecting URLs in Traffic Crossing the Network Boundary	233
Detecting URLs in Network Events	234
Exempting URLs in Network Events	235

Chapter 19: Scanning Files and Other Items 237

How Does CA DataMinder Protect Files on the Local Hard Disk?	237
CFSA Flow Chart: Scanned Files on Local Hard Disk	238
How Does the FSA Scan Stored Data?	239
Which User Policy Gets Applied?	240
Applying Policy to Scanned Items	241
Configure the Local Machine Policy	242
Configure the User Policy	243

Chapter 20: Categorizing Events 249

Overview	249
Why Categorize Events?	251
Categorization Methods	251
How Does Categorization Work?	253
Category Scores	254
How Do Category Scores Affect the Categorization Method?	255
Category Score Summary	256
Guidelines for Categorization Control Triggers and Actions	257
Categorization Trigger Guidelines	258
Do I Need a None of the Above Category?	259
Which Control Action Number?	260
If Both Multi- and Single-Select Email Categorization Actions are Invoked	261
Set Up New Categorization Triggers	261
Add Categorization to Existing Triggers	263
Syntax for Specifying Categories	265
Adding Categories to Existing Triggers	267
Example Category Definitions	268
Smart Tag Category Variables	269
Category Variables	270
Smart Tag Guidelines for Categories and Category Scores	271
Policy Classes	272
Manage Policy Classes	273
Associate Triggers with Policy Classes	273
Trigger Severity	274

Chapter 21: Smart Tagging 275

Overview	275
Set Up a Smart Tag	276
Example Trigger Usage	277
Smart Tags and File Events	278

Smart Tag Names and Values	279
Use Variables as Smart Tag Values	279
X-Headers and Smart Tags	280
X-header Requirements	281
X-header Limitation in Exchange 2003.....	282

Chapter 22: Document Classifications 283

Overview	283
Classification Types	284
Setting Up a Document Classification	284
Setting a File Size Limit	285
Classification in Emails	285
Classification Parameters	285
Parameter 6 Functions	288
Wildcards and Special Characters in Document Classifications	291
Document Classifier Triggers.....	292
Document Classifier Triggers and Key Text	292

Chapter 23: Data Lookup 293

Overview	293
Data Lookup Syntax.....	294
Data Lookup Commands and True-False Tests	295
Add Data Lookup Commands to Control Triggers.....	295
Data Lookup Failure Mode.....	296
Data Lookup Commands and Included, Excluded and Ignored Lists.....	297
User Attribute Lookup	297
User Attribute Lookup Syntax	297
Enable Regionalized Policy Engine Lookup	299
User Attribute Lookup Examples	300
Address Book Lookup.....	301
Address Book Lookup Syntax	302
Address Book Lookup Examples.....	303
Message Attribute Lookup	304
Message Attribute Lookup Syntax	304
Message Attribute Lookup Examples.....	305
XML Attribute Lookup	306
XML Attribute Lookup Syntax	307
XML Attribute Lookup Examples.....	309
XML Metadata Examples	311
Command Variables	313
General Guidelines	314

<Who>	314
<Attribvalue>	317
Labeled <Fallguy>	318
Labeled <Offlimits>	320
<msgvalue>	321
<msgvar>	322
<Numericoperator>	327
<Stringoperator>	327
<Text>	330
<Type>	331
<Uservar>	332
<Xpath>	337
Complex Data Lookup Commands	338
Simple True-False Tests	339
Complex True-False Test	341
Composite True-False Test	341
Complex Composite True-False Test	342
OR and <fallguy> Handling	343
Counting Unique Domains	344
Default List of Long Domains	345

Chapter 24: User Notifications 347

Notification Dialogs	347
Notification Dialog Titles	348
Notification Dialog Messages	348
Copying Text from Notification Messages	349
Notification Emails - Containing Forwarded Emails	350
Replacement Files	350
Variables in User Notifications and Email Replies	351
Variables in User Notifications for File Events	357

Chapter 25: User Definitions 363

Chapter 26: Definitions 364

Chapter 27: Troubleshooting User Policies 367

Triggers Are Not Firing As Expected	367
A Policy is Not Working or Cannot Be Edited	369

Chapter 28: Best Practices	371
Refine Your Policies in a Lab	371
Matching a Document Classification	372
Excluding Emails By Sender	373
Excluding Emails By Subject	375
 Chapter 29: Example User Policy	 377
Example Trigger Settings	378
Example Document Classification	380
 Appendix A: Search Text Syntax	 383
Special Characters	384
Wildcards.....	385
Subexpressions and Logical Operators.....	386
Word and Symbol Variables	387
Number and Money Variables	390
Email Address and URL Variables	392
Repeat Expressions	393
Punctuation Variables	395
Spacing Variables	396
Comments	397
Per Character Matching	398
User-defined Variables.....	400
Transforms	401
TransformEx	402
Validation	403
Matching Forwards and Backwards	405
 Glossary	 407
 Index	 411

Chapter 1: What Is Policy?

This guide provides policy administrators with an overview of user policies, plus instructions and best practice guidelines for editing policies. The guide shows how to edit policies in both the Administration console and iConsole. Other sections describe how to:

- Configure policies to detect key text, email addresses, fingerprinted files, and encrypted data.
- Use text variables when configuring user notification messages and search text expressions.
- Write data lookup commands, including example commands.
- Configure triggers to categorize documents.
- Apply smart tags to events.
- Set up triggers based on document classifications.

Note: This guide uses the terms CA DataMinder Network and Network Boundary Agent (NBA) interchangeably. In particular, this guide uses the term NBA to refer to both the CA DataMinder agent and the Bivio appliance.

This section contains the following topics:

[Introduction](#) (see page 16)

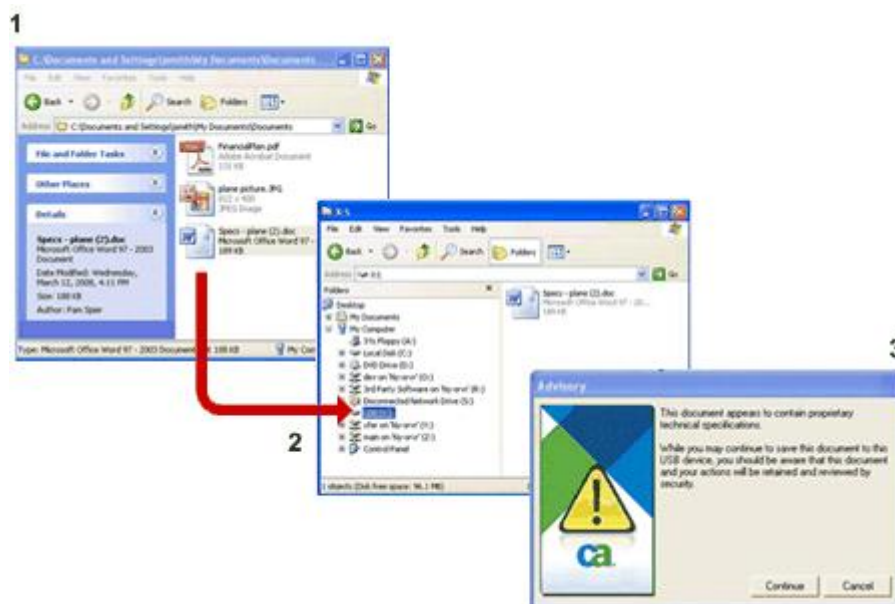
[Who-When-What](#) (see page 17)

Introduction

CA DataMinder user policies can control email, file, and Web activity across your organization. They can also control what applications your users can run and what documents they can print. By editing the settings in a user policy, you have flexibility to control and capture user behavior.

For example, you can block undesirable emails or you can warn the user. You can notify users if an email requires their attention and you can quarantine emails that require a manager's approval. Likewise, you can prevent users from accessing inappropriate Web sites, and even redirect them to an alternative URL. You can also stop users submitting data to a Web site. Similarly, if users try to print or copy sensitive files, you can block or warn against these operations. You can also save a copy of the file for further inspection. If using CA DataMinder to scan stored data, you can delete, move or replace unauthorized documents.

At the endpoint, CA DataMinder can present notifications in a pop-up window. End-users can then use this information provided to complete their current task (for example, by amending an email's content before sending). The notification message is fully customizable and can be as detailed or as brief as needed. The language is also customizable (for example, English for USA and UK employees, and Japanese for employees in Japan).



Example policy intervention: Here, in Windows Explorer, a user attempts to copy a file from their workstation (1) to a USB drive (2). CA DataMinder detects that the file contains sensitive data and displays a pop-up warning (3).

Who-When-What

To better understand how CA DataMinder user policies work, think Who-When-What.

More information:

[Who](#) (see page 17)

[When](#) (see page 17)

[What](#) (see page 19)

Who

Who defines which user is being monitored by CA DataMinder. When CA DataMinder detects unauthorized behavior, or user activity that it needs to control, the first question it asks is ‘Whose policy do I apply?’

For example, if CA DataMinder detects that employee Spencer Rimmel is trying to print an unauthorized file, it applies the policy for Spencer Rimmel’s CA DataMinder account.

Each CA DataMinder user account has its own policy. This policy may be uniquely customized for that person. For example, the Chief Legal Officer may have their own unique policy. More likely, users in the same team or department, or who do the same job, will have policies that are identical. For example, you may want members of the Sales team to all have copies of the same policy.

More information

[Whose Policy Is Applied?](#) (see page 33)

When

When defines the circumstances that cause CA DataMinder to intervene when it analyzes user activity. Remember, CA DataMinder is designed to be as unobtrusive as possible, only intervening when necessary.

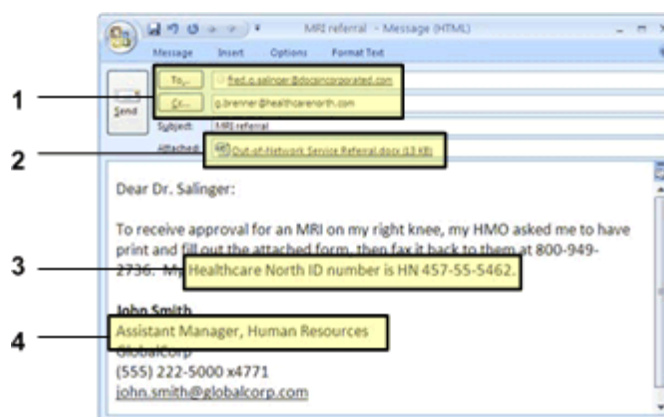
After identifying the user involved, CA DataMinder checks that user’s policy to determine whether to intervene.

For example, if CA DataMinder detects Spencer Rimmel sending an email that contains sensitive information, or sending it to a prohibited address, you can configure his policy to block or quarantine that email.

There are many, many factors that can cause CA DataMinder to intervene, but they broadly divide into two areas:

- **Context:** By context we mean the wider circumstances surrounding an event. For example, if the user is trying to send an email, who are they sending it to? Did they forget to send a copy to their manager? What impact will it have on network traffic? If they are trying to print a file, which printer are they using? If they are copying a document to a USB device, which device is it? And what is its filename?
- **Content:** By content we specifically mean the text content. For example, is the email lacking a corporate disclaimer? Does it use unacceptable language? Does a file or attachment contain confidential information? Has CA DataMinder been able to classify a document (that is, does it match a predefined type or theme, such as a complaint or solicitation)? And if so, do documents matching that classification require special handling?

To define when CA DataMinder intervenes, you must edit the control triggers in your user policies.



Example policy analysis: CA DataMinder triggers analyze an email, checking the addressees (1), any attachments (2), its text content (3). It can also check specific information about the user (4), such as their CA DataMinder account attributes or Address Book properties.

More information:

[What Is in a User Policy?](#) (see page 21)

What

'What' defines the action taken by CA DataMinder after detecting unauthorized activity.

After identifying the user and checking the circumstances to confirm that intervention is required, CA DataMinder can take several possible actions.

For example, it can block Spencer Rimmel's unauthorized email or simply warn him, allowing him to reconsider or rectify what he is doing. Or it can quarantine his email, only releasing it when it has been viewed and approved by Spencer Rimmel's manager. Alternatively, it can cause the email to be encrypted before it is sent.

CA DataMinder can block or warn users from printing a confidential file or copying it to a removable device, network share, or sync folder. CA DataMinder can also encrypt the file before it is copied to a removable device or sync folder.

Likewise, CA DataMinder can block users if they attempt unauthorized Web activity, such as posting a sensitive document or submitting unauthorized comments to a Web site.

If CA DataMinder is scanning a file system (or Exchange Public Folders, or SharePoint site), it can delete, replace or move any unauthorized files or documents that it discovers.

Alternatively, for emails and files, the action taken by CA DataMinder may be to categorize them, allowing them to be easily retrieved from an archive at a later date.

'What' also defines how CA DataMinder notifies a user if it decides to block or warn them, or if it quarantines an email. Typically, users see a pop-up advisory or they receive an explanatory email. The wording is easily customizable to reflect the circumstances that caused the blocking or warning. For example, Spencer Rimmel may see an advisory explaining that his email was blocked because "You are not authorized to send messages to spencer777@hotmail.co.uk pertaining to the Unipraxis acquisition". (In this example, Spencer was trying to send an unauthorized email to his own Hotmail account.)

To define what actions CA DataMinder takes when it intervenes, edit the control actions in your user policies.

Chapter 2: What Is in a User Policy?

This section contains the following topics:

[Summary](#) (see page 21)

[Triggers](#) (see page 21)

[Actions](#) (see page 24)

[System Settings](#) (see page 30)

[Extensions](#) (see page 32)

Summary

A user policy is a collection of settings, stored in a secure tamper-proof file on a CA DataMinder endpoint machine or a CA DataMinder policy engine. These settings fall into the following groups:

- **Triggers:** Define the ‘When’ circumstances mentioned earlier. An individual trigger defines the conditions that cause CA DataMinder to intervene. A single user policy contains hundreds of triggers. You can use as many or as few as you need.

Crucially, each trigger is linked to a policy action. When a trigger fires, CA DataMinder applies the action.

- **Actions:** Define what action is taken by CA DataMinder when a trigger fires. For example, if an unauthorized attachment causes an email trigger to fire, you can configure an action to block the email or warn the user.
- **System Settings:** Control how CA DataMinder applies policy for a specific user or group. The most important system settings are the Document Classifications, Definitions (including User Definitions), and User Notifications. Other system settings are more technical in nature.
- **Extensions:** Determine how often CA DataMinder warns or notifies users that their file or print activity is being monitored.

Triggers

A user policy contains hundreds of triggers, covering all the main channels: incoming and outgoing emails; Web activity; files being copied, printed, or uploaded, or sent over FTP; scanned files; and application usage.

For each channel, there are also separate sets of *control triggers* (these control what a user can do) and *capture triggers* (these save details about what the user was doing).

Email triggers

These control unauthorized attempts to open or send emails. Separate triggers are available for outgoing and incoming emails.

Email triggers can look for such details as: recipient or sender addresses, attachments, whether the email is encrypted, whether it is protected with RMS technology, the absence of a digital signature, and of course, its text content.

Email triggers are used by the following CA DataMinder components:

- Email endpoint agents (Outlook and Notes)
- Email server agents (Exchange and Domino)
- Milter MTA (Sendmail and Postfix)
- Network Appliance (for SMTP and POP3 emails and Webmails such as Hotmail or Yahoo!)
- IIS SMTP agent (for emails transiting through SMTP servers)

Data In Motion Triggers

Data In Motion triggers can control attempts to copy files to removable devices, network locations, and sync folders. They can also control files leaving your corporate network for the Internet and files arriving from the Internet. In addition, these triggers can control HTTP requests, such as attempts to post files or comments to web sites.

Data In Motion triggers can analyze such details as: the names of removable devices or printers, file names and paths or URLs, file properties, whether a file is encrypted or password-protected, and the text content of a file.

The following CA DataMinder agents use Data In Motion triggers:

- Client File System Agent (CFSA)
- Client Print System Agent (CPSA)
- Client Network Agent (CNA)
- Network Appliance (also known as the NBA)
- ICAP Agent

Data At Rest Triggers

Data At Rest triggers can control scanned files or other scanned items. You can also apply them to files imported onto the CMS and files extracted from a third party archive.

Data At Rest triggers can analyze such details as: file names, file properties, whether a file is encrypted or password-protected, and the text content of files.

Data At Rest triggers are used to analyze the following:

- Files scanned by the File Scanning Agent (FSA)
- Files scanned by the Client File System Agent (CFSA)
- Files imported onto the CMS

Application Monitor Triggers

Application Monitor triggers activate when CA DataMinder detects that a user is trying to start a particular application.

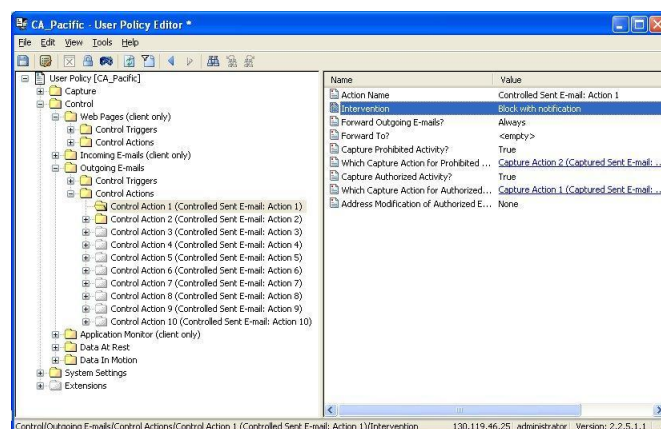
These triggers identify applications by their executable name or their familiar product name—for example, Netscape rather than netscp.exe.

Application Monitor triggers are used by the CA DataMinder Application endpoint agent.

Actions

A user policy contains almost a hundred actions, covering all the main channels (email, Web, files, and so on). For each channel, there are also separate sets of control actions and capture actions.

- A *control action* defines how CA DataMinder intervenes when a control trigger fires. In particular, the *Intervention* setting defines the action you want CA DataMinder to take. For example, if an unauthorized attachment causes an email control trigger to fire, you can configure the Intervention setting to block the email or warn the user. Likewise, if a file scan causes a Data At Rest control trigger to fire, you can, for example, delete the unauthorized file or move it to an approved location.
- A *capture action* determines how much data is captured when a capture trigger fires. For example, you can choose whether to capture Web page images or email attachments.



User Policy Editor, example control actions

More information:

[Email Actions](#) (see page 25)

[Data In Motion Actions](#) (see page 26)

[Data At Rest Actions](#) (see page 27)

[Application Monitor Actions](#) (see page 28)

[Control Action Precedence](#) (see page 29)

Email Actions

You have enormous flexibility to control emails. Control actions enable you to block specified emails, or simply show a warning to the sender or intended recipient. You can encrypt unencrypted outgoing emails. You can also quarantine and categorize emails. You can even silently monitor email traffic. CA DataMinder supports the following actions:

- **Blocking emails:** You can block specific *outgoing emails*. When this happens, CA DataMinder displays an advisory dialog or sends an explanatory email to the sender. You define the message that the sender sees. In fact, you can define separate messages for each control trigger.

You can also block *incoming emails*. If required, you can discreetly block the email so that the intended recipient is unaware that their email has been blocked. Or you can replace the email body text with a pre-defined notification. In both cases, you can send an automatic reply to the sender, containing an explanatory message.

- **Warning users:** If required, you can warn users when they try to send or open an unauthorized email. A warning dialog lets the user choose whether to continue or not.

If the user chooses to continue, they are allowed to send (or open) the email, but CA DataMinder records the fact that they did this despite being explicitly warned against doing so.

- **Encrypting emails:** You can set up an Outgoing Email control action to add an 'encryption request' x-header to an outgoing unencrypted email. This x-header indicates to third-party encryption providers that the email must be encrypted before it is sent.
- **Quarantining emails:** You can quarantine outgoing emails that require urgent review. You can optionally notify the sender that this has happened. Reviewers can subsequently release the email from quarantine (sending it to its intended recipients) or reject it (the email is not sent).
- **Informing or notifying users:** If required, you can display an advisory dialog whenever CA DataMinder detects an email that may be significant. This is useful if you want to notify users when specified emails arrive in their Inbox or you want to inform senders that their email is missing a disclaimer.
- **Silent monitoring:** If required, you can silently record each occurrence when an email triggers a control action, but without blocking the email or displaying a warning. The user is completely unaware that their email triggered a control event.
- **Categorizing emails:** You can set up a control action to categorize emails. You define the categories in email triggers (for example 'internal memo' or 'humorous'). You can specify that categorization is automatic or manual. If you want users to categorize their own emails, you can configure a control action to display a notification dialog listing the available categories.

- **Forwarding emails:** You can forward an email to another address. For example, if any user disregards a warning and sends an unauthorized email, you can forward a copy to your Compliance Officer. The Compliance Officer then receives a standard notification email with the original email included as an attachment.
- **Automatic replies to incoming emails:** For any incoming email, you can send an automatic reply to the sender. You choose what information is included in the reply.
- **Capturing emails:** Email *capture actions* let you capture the associated email or attachment, or capture details about the event. These details include the user name, when the trigger was activated, and so on.

Any email *control action* can also invoke a capture action.

Data In Motion Actions

Data In Motion actions let you control files being moved across a network, copied to removable devices or sync folders, or sent to a printer. They can also control HTTP requests, such as attempts to post files or comments to web sites.

In most cases, you can block and categorize the files. For files being copied to removable devices, network locations, and sync folders, you can also force or advise users to encrypt unencrypted files. The full range of actions is summarized below.

- **Blocking files:** You can block a file or document. The blocking is either silent, or the user is shown an advisory dialog.

When a file is blocked, CA DataMinder displays an advisory dialog. For example, the advisory is shown if a user tries to print an unauthorized file or copy it to a USB device.

Note: For files blocked by the NBA, the blocking is silent. That is, no advisory is shown.

- **Warning users:** If required, you can warn users when, for example, they try to print a file. If the user chooses to continue, CA DataMinder records the fact that they did this despite being explicitly warned against doing so.

Note: Warnings are not supported for events detected by the NBA or Client Network Agent.

- **Encrypting files:** You can set up a control action to encrypt an unencrypted file when a user attempts to copy it to a target such as a removable device or sync folder. CA DataMinder also copies an encryption utility to the target. This utility enables the user to decrypt the file when they want to copy it from the target onto another computer.

Note: CA DataMinder cannot encrypt files being copied to network locations. Do not use Advise Encryption or Enforce Encryption control actions to prevent unencrypted files being copied to shared locations on your network.

- **Categorizing files:** You can set up a control action to automatically categorize files. You define the categories in Data In Motion triggers (for example 'Sales Contract').
- **Silent monitoring:** If required, you can silently record each occurrence when an file triggers a control action, but without blocking the file or displaying a warning. The user is completely unaware that their activity triggered a control event.
- **Capturing files:** Data In Motion *capture actions* let you specify how much file detail is captured. For example, you can capture the file itself, or just its metadata (file attributes), or both.

Any Data In Motion *control action* can also invoke a capture action.

Data At Rest Actions

Data At Rest actions let you control scanned and imported files. You can delete specified items, replace them with explanatory 'stub' files, copy or move them to a new location, or simply categorize the files. CA DataMinder supports the following actions:

- **Deleting files:** If required, you can silently delete scanned files. From a user's viewpoint, they will only be aware that their file no longer exists when they next try to view it. You can still capture, copy or move the original file.
- **DoD Overwriting and Deleting:** You can use DoD deletions to ensure deleted files cannot be recovered. From a user's viewpoint, they will only be aware that their file no longer exists when they next try to view it. You can still capture, copy or move the original file.

DoD deletion is forensic deletion, so called because the storage media are purged to guarantee that a file cannot be recovered and used to obtain evidence in legal discovery. DoD refers to the U.S. Department of Defense approved methods for purging storage media.

- **Replacing files:** You can delete scanned files and replace them with an explanatory stub file to alleviate any user concerns. This explanatory message is defined in the Data At Rest trigger. For example, you can inform a user that their file was inappropriate and has been removed to a new location. You can still capture, copy or move the original file.
- **DoD Overwriting and Replacing:** You can use DoD deletions to delete files and replace them with an explanatory stub file. You can still capture, copy or move the original file.
- **Moving or copying files:** You can copy scanned files to an alternative location. You can combine Copy and Delete operations to effectively move scanned files to a new location.
- **Categorizing files:** You can set up a control action to automatically categorize files. You define the categories in Data At Rest triggers (for example 'Sales Contract').

- **Capturing files:** Data At Rest *capture actions* let you specify how much file detail is captured. For example, you can capture the file itself, or just its metadata (file attributes), or both.

Any Data At Rest *control action* can also invoke a capture action.

Application Monitor Actions

You can use these actions to control which applications users are permitted to run. You can block unauthorized applications or warn users when they try to run, for example, Firefox or Chrome.

Control Action Precedence

An event can fire multiple control triggers and each trigger can potentially fire a separate control action. The order in which multiple control actions are applied out is determined by the control action number. That is, the control action with the lowest number takes precedence—see example below. This has important implications for the Intervention setting. For example, if a Warning control action takes precedence over a Blocking control action, the event generates a warning but is not necessarily blocked.

Note: This also has important implications for quarantine events.

Example

If an email causes three control triggers to activate (Attachment, Recipient and Search Text), then these triggers respectively invoke control action 5, control action 2 and control 3, with control action 2 being applied first. The only action invoked against the event will be Control Action 2, because after an event is blocked, no other actions can be invoked.

- A Recipient trigger invokes **Control Action 2: Blocking**. This control action is applied **1st**.
- A Search Text trigger invokes **Control Action 3: Quarantine**. This control action is applied **2nd**.
- An Attachment trigger invokes **Control Action 5: Warning**. This control action is applied **3rd**.

Intervention options

This section summarizes how intervention options affect any subsequent control actions:

- If a Blocking occurs, no other actions are invoked subsequently.
- If a Warning occurs and the user clicks Cancel, no other actions are invoked subsequently.
- If a Warning occurs and the user clicks Continue, the next control action is invoked.
- If a Quarantine control action occurs, no other actions are invoked subsequently.
- If a Silent control action occurs, the next control action is invoked.

Quarantine control actions

Important! Use the *highest* number control action as your Quarantine control action in order to give it the *lowest* priority.

The precedence of control actions has an important effect on quarantined e-mails. If an email causes a control trigger to fire, which then invokes a quarantine control action, the email is exempt from further control actions. That is, a quarantined email cannot also be blocked or generate a warning.

We therefore recommend that you use highest control action as the Quarantine control action. For example, if there are 10 control actions, configure Control Action 10 as the Quarantine control action.

This means that if an email causes multiple control triggers to fire, invoking multiple control actions, the quarantine control action is applied to the email last. This allows other control actions, such as warnings, to be invoked first. For example if a user sends an email containing bad language, you may want to warn the user. If he or she ignores the warning, you can then quarantine the message.

System Settings

System settings control how CA DataMinder implements policy for a specific user or group. The most important system settings are the Document Classifications, Definitions (including User Definitions), and User Notifications. Other system settings are more technical in nature and include, for example, data lookup timeouts.

Document Classifications

Document Classifications are important because they enable CA DataMinder to detect documents (emails, attachments, files and Web pages) with specific themes, for example, a contract agreement or customer complaint.

You can set up triggers to use a specific document classification. Email, Web, Data At Rest and Data In Motion triggers all support document classifications. When the trigger activates, CA DataMinder compares the active document (for example, this could be an email or a printed file) against the specified classification. If it confirms the match, a policy action is invoked.

Each document classification uses parameters to identify a specific document type defined by you for example, a contract agreement. These parameters contain the rules that enable CA DataMinder to identify this type of document. When classifying a document, CA DataMinder calculates a document score, based on the classification parameters. It uses this to quantify the probability that, for example, a file really is a contract agreement.

Definitions

The system settings include a Definitions subfolder. Settings in this subfolder let you specify various definitions, such as internal email address patterns, archive file extensions, and 'user definitions' (variables defined by you, such as a list of banned phrases).

Such user definitions can be referenced by any setting in the current policy that takes a text value (such as trigger names, address lists, search text lists, and messages to users). This can save time and ensure consistency if a policy contains many settings that use the same.

Example

For example, you can add a 'Disclaimer' user definition and set its value to:

Unipraxis distributes this document for informational purposes only.

You can then reference this definition as %Disclaimer% in any other policy trigger. For example, you can include this definition in the explanatory message that users see when their email is blocked, for example:

"Your email has been blocked because it does not include the mandatory corporate disclaimer: %Disclaimer%"

User Notifications

The system settings include a User Notifications subfolder. Settings in this subfolder determine the titles for advisory dialogs shown when user activity triggers a blocking or warning. They also determine the subject and body text for notification emails containing a forwarded email.

Other System Settings

These are generally more technical in nature. The main groups are summarized as follows:

- **Email Encryption Settings:** You can set up outgoing email control actions to flag emails for encryption by a third-party encryption provider. These settings identify the encryption providers plus the 'flag for encryption' x-headers inserted into emails by CA DataMinder and recognized by these providers.
- **Text extraction:** Several settings control how CA DataMinder extracts text when analyzing the content of an email or document. For example, to avoid processing delays you can specify a maximum file size; CA DataMinder will not try to analyze files above this limit.

- **Sender and recipient handling:** Other settings control how CA DataMinder handles sender and recipient details in emails. For example, to alleviate delays when analyzing emails sent to very large distribution lists you can specify a maximum number of list members.
- **Data Lookup timeouts:** You can set timeouts to prevent complex triggers taking too long to activate. For example, if trigger needs to look up a user's attributes in the CMS database, you can specify how long it waits for the CMS to reply.

Note: Data Lookup commands are included in Email, Data At Rest and Data In Motion control triggers. They allow the trigger to test some aspect of the event. For example, they can look up an Outlook Address Book property of an email recipient. They can also be used to test a file's metadata, such as its Creation and Last Modified dates.
- **Sensitive information handling:** These settings control the handling of passwords and credit card numbers captured by CA DataMinder. They enable you to conceal captured so they are not readable in the iConsole.

Extensions

Extensions settings focus on messages to notify users that their activities are being monitored. Settings determine the message content and how often the message is displayed. For example, Client Print System Agent settings define the message seen by users when they press the Print Screen button (if the button is disabled).

Chapter 3: Whose Policy Is Applied?

When CA DataMinder detects unauthorized behavior or activity that it needs to control, the first question it asks is 'Whose policy do I apply?' To answer this question, CA DataMinder must map the user to a CA DataMinder user account. The mechanism for doing this depends on the type of activity.

This section contains the following topics:

[Email Activity](#) (see page 33)

[File Monitoring and Scanning](#) (see page 34)

[Printed Documents](#) (see page 35)

[Web Activity](#) (see page 35)

[Application Monitoring](#) (see page 36)

[Internal and External Email Addresses](#) (see page 36)

[Exempt Users](#) (see page 38)

Email Activity

CA DataMinder associates emails with users depending on how and where CA DataMinder detected the email (the 'capture source').

- **Email endpoint agents:** When CA DataMinder detects emails in Outlook or Notes, it associates the user's Windows logon credentials with a matching CA DataMinder user account and applies that user's policy. That is, CA DataMinder can identify the user sending (or receiving) an email and apply that user's policy to the email.

The synchronization between Windows accounts and CA DataMinder accounts is created in the CMS database during an Account Import job or, less commonly, by using Microsoft Windows user authentication to automatically generate new user accounts.

- **Email server agents:** For emails detected as they pass through Exchange, Domino or Sendmail servers, CA DataMinder first determines whether the sender's email address matches an internal address pattern. If it does and the sender corresponds to an existing CA DataMinder user account, that user's policy gets applied.

If no matching CA DataMinder user can be found, or if the sender is deemed to be external, then CA DataMinder applies either the 'unknown internal sender' policy or the 'external sender' policy. These are CA DataMinder user accounts set up specifically for this purpose.

- **Network Appliance:** For emails sent across your corporate network to or from the Internet, passing through the CA DataMinder Network Appliance, CA DataMinder tries to map the sender's email address to a CA DataMinder user account.

However, because the Network Appliance typically targets messages sent from private Webmail accounts, in many cases it will not be possible to map the sender's address to a CA DataMinder account. In this situation, CA DataMinder applies either the 'unknown internal sender' policy or the 'external sender' policy.

File Monitoring and Scanning

It is often difficult to reliably match a captured file or scanned item to the actual author or creator of the file. In this situation, CA DataMinder typically applies the policy for a 'system' user account (such as the Default Policy For Files) rather than the policy for an actual user. However, the actual method used to associate files with a CA DataMinder user account depends on the capture source:

- **Event Import:** You can configure import jobs to associate imported files with specific CA DataMinder users. In particular, the `ImpFile.PolicyParticipant` import parameter determines whose policy gets applied to imported files. In fact, this parameter specifies an email addresses. Linked tables in the CMS database enable CA DataMinder to map this address onto an existing CA DataMinder user accounts.

If no matching CA DataMinder user can be found, then CA DataMinder applies the 'Default Policy For Files'. This is a CA DataMinder user account set up specifically for this purpose; it is defined in the policy engine's machine policy. It defaults to the `DefaultFileUser`; this is a CA DataMinder user account created automatically when you install a CMS.

- **File Scanning Agent (FSA):** When the FSA runs a scanning job, the job definition determines which user's policy is applied to scanned files. You can either specify the Default Policy For Files (see above) or an email address.

If you specify an email address, CA DataMinder maps this address onto an existing CA DataMinder user account. As for imported files, if this mapping files then CA DataMinder applies the Default Policy For Files.

- **Network Appliance (formerly NBA):** The Network Appliance can capture files being sent across the Internet boundary. These include downloads, uploads, FTP transfers, and email attachments. The mechanism for associating these files with CA DataMinder users depends on which mode the Network Appliance is running in. When it runs in:
 - **Socket output mode:** The Network Appliance passes captured files to policy engines for processing. The policy engine always applies the Default Policy For Files (see above).
 - **Disk output mode:** The Network Appliance saves captured files to the local disk. These files are subsequently imported onto the CMS using Event Import. You then configure the import job using the ImpFile.PolicyParticipant parameter (see above) to determine whose policy gets applied to imported files.
- **Client File System Agent (CFSA):** When the CFSA detects a user copying a file to a removable device or network location, it associates the user's Windows logon credentials with a matching CA DataMinder user account and applies that user's policy. The synchronization between Windows accounts and CA DataMinder accounts is the same as for CA DataMinder email endpoint agents.

When the CFSA scans the local hard disk, it applies the 'Default Policy For Data At Rest'. This is a CA DataMinder user account set up specifically for this purpose; it is defined in the client machine policy. It defaults to the DefaultClientFileUser; this is a CA DataMinder user account created automatically when you install a CMS.

Printed Documents

When the Client Print System Agent (CPSA) detects a user trying to print a document, it associates the user's Windows logon credentials with a matching CA DataMinder user account and applies that user's policy.

The synchronization between Windows accounts and CA DataMinder accounts is the same as for CA DataMinder email endpoint agents.

Web Activity

Web events are captured by the Client Network Agent . The agent associates the user's Windows logon credentials with a matching CA DataMinder user account and applies that user's policy.

The synchronization between Windows accounts and CA DataMinder accounts is the same as for CA DataMinder email endpoint agents.

Application Monitoring

Application events are captured by the CA DataMinder Application endpoint agent. The agent associates the user's Windows logon credentials with a matching CA DataMinder user account and applies that user's policy.

The synchronization between Windows accounts and CA DataMinder accounts is the same as for CA DataMinder email endpoint agents.

Internal and External Email Addresses

CA DataMinder can identify emails sent to or from internal or external addresses. This is useful for two reasons. First, you can set up policy to control emails being sent to external recipients (for example, because your organization operates an 'Internal Use Only' email policy). Second, you can search in the iConsole for incoming and outgoing emails. This allows you to identify trends and patterns in email traffic entering and leaving your organization.

Identifying Internal and External Senders

CA DataMinder can identify emails where the sender is internal or external. How it does this depends on whether the email was captured by an endpoint agent or server agent.

Emails captured by endpoint agents

By definition, the sender of an email detected by the Outlook or Notes endpoint agent must be internal. This is because, when the email is sent, CA DataMinder has already associated the sender's Windows logon credentials with a matching CA DataMinder user account. In effect, it recognizes the sender.

Emails captured by server agents

When an email server agent (such as the Exchange or Domino agent) detects an email, they need to determine whether the sender is internal or external. This analysis is handled by a CA DataMinder policy engine (PE).

Specifically, the PE uses these settings in its *machine policy* to determine which *user policy* to apply:

Internal Email Address Pattern

Specifies a list of internal email address patterns, such as '@unipraxis.co*'. When a PE receives an email for processing, it first compares the sender's address against the listed address patterns:

If a match is confirmed, the sender is deemed internal. The PE then checks whether the sender's address matches an existing CA DataMinder user's address. If it does, the PE applies that user's policy; if not, the PE applies the Unknown Internal Sender's policy (see below).

If the sender's address does not match an internal address pattern, the sender is deemed external and the PE applies the External Sender's policy.

Unknown Internal Sender

Policy engines use this setting to apply policy to emails sent within the organization from unrecognized users. It defaults to 'UnknownInternalSender'; this user account is created automatically when you install a new CMS.

External Sender

Policy engines use this setting to apply policy to external emails. That is, emails sent from someone outside the organization. It defaults to 'ExternalSender'; this user account is created automatically when you install a new CMS.

Exempting Internal Emails From Policy

If you want to block emails sent outside the company (to external recipients), you can make a simple change to the user policy to exempt internal addresses but block external addresses. To do this, edit this user policy setting:

Excluded Addresses

Find this setting in each of your Outgoing Email triggers. When you edit this setting, add a list of internal addresses and domains as follows:

- If an email recipient matches an excluded address (because the recipient is internal), the email is exempted and policy is not applied.
- If the recipient does not match an excluded address, CA DataMinder infers the recipient is external and applies policy to the email.

Flagging Emails As Internal

If you want to flag emails as internal or external, you can define a list of internal email addresses. Any addresses not on the list are deemed to be external.

CA DataMinder classifies an email as internal only if the sender and all recipients have internal email addresses. If an external address is detected, it flags the email as external.

This feature serves two purposes:

- It allows you to search in the iConsole for internal or external emails and inbound or outbound emails (that is, e-mails entering or leaving your organization).
- It allows you to selectively apply policy to emails sent outside your organization. For example, you can quarantine an email sent to multiple external recipients, but allow the email if it is only sent to a single external recipient. To do this, you set up your Outgoing Email triggers to use message attribute lookup commands to count the number of internal or external recipients.

In both cases, this feature depends on a list of internal addresses being defined in your user policies. Specifically, you need to edit this user policy setting:

Internal Emails

Find this setting in the System Settings, Definition folder. When you edit this setting, add a list of internal addresses and domains.

Exempt Users

(Only applicable for users with licenses such as CA DataMinder Express)

Exempt users are users who have a CA DataMinder account on the CMS but who are exempt from policy. That is, CA DataMinder does not monitor email, web or file activity for policy-exempt users.

Most importantly, exempt users are not included in your licensed user count. For example, if your CA DataMinder license allows 100,000 users, your CMS is permitted to store user accounts for 100,000 licensed users *plus* an unlimited number of exempt users.

Why Do I Need Exempt Users?

If you deploy CA DataMinder endpoint agents on a shared computer (for example, in a hot desking environment), a new CA DataMinder user account is created automatically each time a new user logs onto that computer. In an organization with many shared computers, this can result in more user accounts than your CA DataMinder license permits. In turn, this can mean that some users are not subject to policy control even if you want them to be.

Even if you delete an unwanted CA DataMinder account in the Administration console, CA DataMinder automatically recreates the account if that user logs into Windows again on any CA DataMinder computer.

If you have users in your organization who are not subject to CA DataMinder policy control, you can exempt these users from policy to avoid exceeding your maximum number of licensed users.

How Do I Create Exempt Users?

You can manually exempt users from policy. In effect, you convert a licensed user account to an exempt user account.

You can also automatically exempt specific users from policy when you run an Account Import job. For example, you can exempt any user accounts imported from your LDAP directory and which have a specific LDAP attribute.

Manually Exempt Users From Policy

You can manually exempt users from policy. You can also manually undo a policy exemption.

To exempt users from policy

1. Log on to the Administration console using an account that has the 'Users: Edit the user hierarchy' administrative privilege.
2. Expand the User Administration branch and select the users who you want to exempt from policy.
3. Click Tools, Set Policy Exemption.
The Select Policy Exemption State dialog appears.
4. Select the Exempt From Policy check box and click OK.

To undo a policy exemption

1. Log on to the Administration console using an account that has the 'Users: Edit the user hierarchy' administrative privilege.
2. Expand the User Administration branch and select the policy-exempt users who you want to apply policy to.
3. Click Tools, Set Policy Exemption
The Select Policy Exemption State dialog appears.
4. Clear the Exempt From Policy check box and click OK

Chapter 4: How Policy Works

This section contains the following topics:

[Policy Processing](#) (see page 41)

[Policy Inheritance](#) (see page 45)

[Policy Version Numbers](#) (see page 47)

[Policy Folders and Settings](#) (see page 49)

[Controlling Policy Changes](#) (see page 55)

Policy Processing

Every day, CA DataMinder server and endpoint agents analyze thousands of events. Most of these are benign and do not need to be under policy control. So how does CA DataMinder separate those events that require policy from those that do not without causing massive disruption to an organization's daily work?

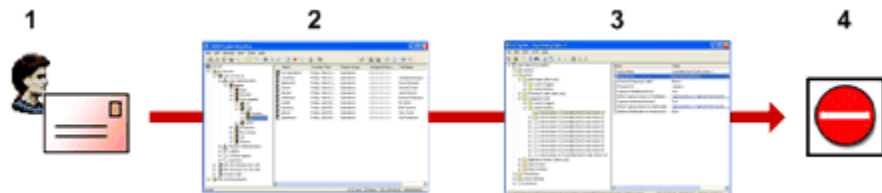
When CA DataMinder detects an event, whether it is an email, IM conversation, a print job, or a file, it goes through the following steps:

1. First, it identifies the **event owner**. For example, this may be the sender of an outbound email.
2. After identifying the owner, it associates the owner with a CA DataMinder **user account**.

Typically, each employee has their own user account. If CA DataMinder identifies an employee as the event owner, it can quickly locate that employee's user account.

For events that cannot be associated with an employee, such as emails sent from outside your organization or files stored on your network, CA DataMinder typically assigns a default owner. This default owner corresponds to a 'system' user account (such as the External Sender or DefaultFileUser) rather than the policy for an actual user.

This process of associating the owner (1) with a CA DataMinder user account is very fast. Each CA DataMinder policy engine contains a record of the entire user hierarchy (2), and this record is continually kept up to date. Each endpoint agent identifies the relevant user account when the user first logs on. CA DataMinder applies that account's user policy to the event.



Policy processing procedure: CA DataMinder associates the event owner (1) with an account in the CA DataMinder user hierarchy (2). It then applies this account's policy (3). If a policy trigger fires, it immediately applies the appropriate action, such as a blocking (4).

3. After locating the correct account in the user hierarchy, CA DataMinder applies that account's **user policy** to the event as follows:
 - a. If the policy engine or (this is unlikely) the endpoint agent does not already hold a cached copy of the required user policy, it requests the policy from the CMS.
 - b. CA DataMinder then identifies the relevant triggers within this policy. For example, if CA DataMinder is scanning a file system, it knows that it only needs to apply Data At Rest triggers. All other trigger types are immediately disregarded. It also immediately disregards all disabled triggers.
 - c. Finally, it tests all the relevant triggers. That is, it applies each trigger to see whether the event causes the trigger to fire. Triggers are applied in the order in which they are listed in the user policy.
4. When CA DataMinder applies an individual trigger, it tries to determine as fast as possible whether the trigger will fire. It therefore applies the simplest, fastest trigger criteria first. If an event fails to match these criteria, CA DataMinder knows that the event is benign and can be exempted from further policy processing. CA DataMinder then applies the next trigger listed in the user policy.
5. After applying all the relevant triggers, CA DataMinder applies the corresponding control actions if one or more triggers fired (if no triggers fired, no actions are applied).

It applies the control actions in order of priority. The order in which multiple control actions are applied is determined by the control action number. The control action with the lowest number takes precedence. For example, Action 1 always gets applied before Action 2 or Action 3.
6. When all control actions have been performed, CA DataMinder then performs any required capture actions.

Applying Triggers to Emails

When CA DataMinder applies a trigger to an email, it does the following:

1. It analyzes the event metadata, including sender and recipient details. For example, is the email being sent to an authorized recipient?
2. It performs any Message Attribute or XML Attribute data lookups. These lookups can quickly tell CA DataMinder whether to fire a trigger. For example, a trigger may be configured to always fire if an email has more than 10 recipients.
3. It analyzes the text content of the email, starting with the subject and then the body text (if required).
4. If CA DataMinder is unable to determine whether to fire the trigger, it performs any 'remote' data lookups, that is, User Attribute lookups and Address Book lookups. These are 'remote' lookups because CA DataMinder must retrieve the information respectively from your CMS or your preferred LDAP server (typically your Active Directory host).

Applying Triggers to Files

When CA DataMinder applies a trigger to a file, it does the following:

1. It analyzes the file metadata. In most cases, this only includes the name of the file.
For example, a Data At Rest trigger may exclude all bitmaps (*.bmp files) from policy. As soon as CA DataMinder detects a bitmap, it knows to exempt the file from further policy processing.
2. It analyzes the content of the file. For example, it can compare the file against document classifications or it can check for keywords or phrases.

Applying Triggers to Web Events

When CA DataMinder applies a trigger to a Web event, it does the following:

1. It checks the URL. For example, users may be prohibited from browsing certain URLs.
2. It analyzes the available text content. This may be text on a Web page or the content of a file upload.

Applying Triggers to IM Conversations

When CA DataMinder applies a trigger to an IM conversation, whether detected by the NBA or imported from an archive, it handles each posted comment like an email and each file attachment as if it were an FTP file transfer.

This means that it applies each participant's policy to any comment they post or any file they attach. In practice, this means that CA DataMinder analyzes the text content of each comment for key words or phrases. For file attachments, it first checks the file name and then analyzes the text content.

Optimized Policy Processing

CA DataMinder is designed to minimize the level of policy processing needed to accurately analyze an event.

Policy processing is optimized to ensure that triggers are accurately applied as quickly as possible. In particular, these optimizations ensure that no unnecessary processing is performed, and that processing terminates correctly at the earliest opportunity. For example, CA DataMinder supports the following optimizations:

- A Block action terminates policy processing. No further control actions get applied after an event is blocked. The same is true for Warning events where the user heeds warning. That is, if a user heeds a warning and does not continue, no further control actions are applied.
- CA DataMinder supports a No Further Action intervention option. This is primarily used to handle spam emails. This option instructs CA DataMinder to immediately stop processing an event and ensures that any subsequent actions which would normally be performed (such as forwarding the email or sending a reply) are not performed.
- CA DataMinder uses a data-on-demand approach when transferring policy settings across the network. If a policy engine requires policy data from the CMS *while processing an event* (that is, it does not have a cached copy of the required user policy), the CMS only sends the minimum data necessary to complete each processing step.

For example, if a policy engine needs a user's email policy to be sent down from the CMS, the CMS at first only sends those trigger settings that analyze the email's metadata. If these settings are sufficient by themselves to fire the trigger (for example, because the email is addressed to a proscribed recipient), then no further policy settings get sent across the network.

Policy Inheritance

Most enterprises need many different policies to support the diverse needs of users. For example, different departments and various levels of management might each require their own, customized policy. To streamline policy administration, CA DataMinder uses automatic policy inheritance. This enables you to quickly administer large numbers of users.

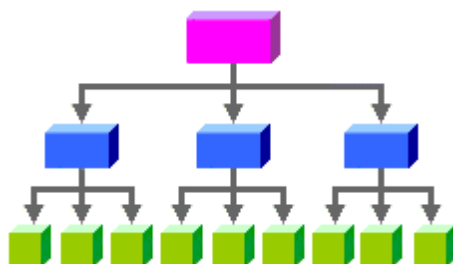
Policy inheritance operates in two dimensions. First, attributes are inherited within a policy branch. Second, there is inheritance from parent to child policies.

Parent-Child Policy Inheritance

This means that a child policy inherits folder attributes and values for individual settings from a parent policy. That is, the value for any setting passes automatically from a parent policy to the equivalent setting in a child policy. Likewise, the attributes defined for any folder pass automatically to the equivalent folder in a child policy.

By default, any change made to a setting in a parent policy is automatically applied but not enforced in a child policy. However, you can optionally enforce these changes in child policies.

For users, parent and child policies derive from the hierarchy of user groups defined in the Administration console. This means that group policies are always parent policies, because their settings are passed on to all users in the group. Likewise, policies for individual users are always child policies, and cannot be inherited by another user. But a group policy is also usually a child policy, because it inherits its settings from a higher-level user group. (Ultimately, all group policies derive from a master policy defined for the top-level 'Users' group.)



■ Master policy
 ■ Group policy
 ■ User policy

More information:

[Policy Inheritance](#) (see page 45)

[Enforcing Modified Settings in Child Policies](#) (see page 53)

Policy Branch Inheritance

A policy branch refers to all policy folders and settings contained within the current folder.



Within a policy branch, the **Hide** and **Disable** attributes for a parent folder are inherited by all its subfolders and setting. For example, if a folder (1) is hidden, its subfolders and settings are all also hidden (2):



An inherited attribute is not the same as an attribute that is explicitly set. For example, un hiding a parent folder will not unhide settings within that parent folder, which have been hidden directly. (You can check this in the Properties dialog. For any setting that has been hidden directly, the attribute check box is selected in the Properties dialog: ☒ **Hide from users**. Conversely, for settings that are disabled simply because their parent folder is disabled the check box is clear in the Properties dialog: ☐ **Hide from users**.)

Note: The **Enforce** attribute is exempt from automatic policy branch inheritance. When you enforce a folder, this only enforces settings within the current folder and within the equivalent folder in any child policies.

More information:

[Policy Inheritance](#) (see page 45)

[Enforced Folders and Policy Branch Inheritance](#) (see page 52)

Policy Version Numbers

Each time a policy is edited, the relevant value in its version number increments by +1. Policy version numbers allow administrators to track local and inherited policy updates.

When you select a user, group or machine in the Console, the attributes in the right-hand pane show the policy version. Version numbers contain a series of dot-separated values, for example:

1.2.5.3

Each value represents the policy version at a specific level in the user or machine tree.

- **1st value** This shows the version of the policy licensed for your organization. When you install a new license file, this value increments by +1 (1.2.5.3 to 2.2.5.3).
- **2nd value** This shows the version of the master policy for your organization. When you upgrade CA DataMinder, this value increments by +1 (1.2.5.3 to 1.3.5.3).
- **3rd value** For user groups, this shows the policy version for the top level 'Users' group. For machines, it shows the policy version for the CMS. These policy edits increment the value by +1 (1.2.5.3 to 1.2.6.3).
- **4th and subsequent values** For users and groups, this shows the policy version of a next-level user group or user. For machines, it shows the policy version of a next-level gateway or client machine. These policy edits increment the value by +1 (1.2.5.3 to 1.2.5.4).

Policy Version Example

In this user policy example, numbers in brackets (4) indicate the policy version values at that level in the user tree:

Licensed policy for your organization: (1)



* Corresponds to the master policy for your organization.

- 1 Initially, this gives the following policy versions:

Group: Users	1.2.4
Group: Directors	1.2.4.1
User: frankschaeffer	1.2.4.1.1
User: spencerrimmel	1.2.4.1.3

2 If you then edit only the Directors group policy, this gives:

Group: Users	1.2.4 (no change)
Group: Directors	1.2.4.2
User: frankschaeffer	1.2.4.2.1
User: spencerrimmel	1.2.4.2.3

3 Finally, if you edit the policy for spencerrimmel, this gives:

Group: Users	1.2.4 (no change)
Group: Directors	1.2.4.2 (no change)
User: frankschaeffer	1.2.4.2.1 (no change)
User: spencerrimmel	1.2.4.2.4

Reported and Assigned Policy Versions

When rolling out policy changes across your organization, it is important to understand the difference between **reported** and **assigned** policy versions.

Reported policy version

The version of a policy reported by a client machine to the CMS when it logs on to CA DataMinder.

Assigned policy version

The latest policy version held on the CMS. This version is automatically replicated to the relevant client machine at intervals determined in the CMS policy.

Why do reported and assigned versions differ?

This can happen if an administrator updates a user's policy while the user is not logged on to CA DataMinder. In this situation, the updated (or assigned) policy is held on the CMS but the old policy remains on the client machine. When the user next logs on to CA DataMinder, their client machine reports that it is using the old policy. Eventually, the discrepancy is eliminated when the assigned version of the policy replicates down from the CMS to the client machine.

Policy version mismatches can also occur if two people are logged on to separate client machines as the same user. In the Administration console, the policy versions shown for that user account are those of the person who connected most recently to the CMS. If an administrator then updates that user's policy, the assigned policy is replicated down to the client machines. There may be a few seconds delay before the policy versions shown in an Administration console update to the latest version.

Note: You can view the reported and assigned policy versions for individual users  in the Administration console. If a user is logged on to CA DataMinder, you can select the user and view their Open Session details in the right-hand pane. These include both policy versions.

Policy Folders and Settings

Each policy folder and setting can have any combination of three attributes: disabled, enforced and hidden. These attributes, in combination with policy inheritance, let you tailor the scope of any custom policies that might be needed lower down your hierarchy of machines or users.

Disabled Policy Folders

When a folder is disabled, CA DataMinder ignores all settings in the folder and its subfolders. For example, if you disable the URL triggers for Web pages folder, a URL alone cannot cause a trigger to fire.

You cannot disable individual settings, but settings become disabled when their parent folder is disabled. A folder might have been disabled directly. More commonly, a folder is disabled because its parent folder has been disabled. Alternatively, the equivalent folder might have been disabled in the parent policy. In this last case, you can only re-enable the folder by re-enabling the equivalent folder in the parent policy.

Disabling a Folder

To disable a folder

1. In the Policy Editor, select a folder.
2. Click  or right-click and choose Disabled.

To re-enable a disabled folder

1. Select a disabled folder.
2. Click  or right-click and choose Disabled.

Note: Certain essential policy folders can never be disabled. For example, this applies to all settings in the machine policy. Also, you cannot re-enable a folder if:

- Its parent folder in the same policy is still disabled.
- The equivalent folder is disabled and also enforced  in the parent policy. The Enforce attribute, when applied to a folder, prevents anyone re-enabling the folder in a child policy.

More information:

[Policy Inheritance](#) (see page 45)

[Conceal Disabled Folders](#) (see page 51)

Conceal Disabled Folders

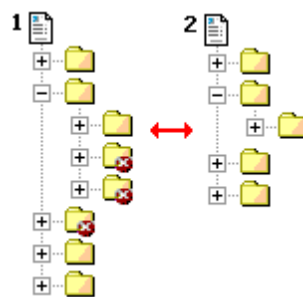
If you disable folders in a policy, it can be hard to focus on the effective policy areas. To only focus on those folders that remain enabled, configure the Policy Editor so it does not display disabled folders.

To conceal disabled folders

Choose View, Show Disabled Items to conceal these folders. Or press Ctrl+D.

To show disabled folders

Choose View, Show Disabled Items. Or press Ctrl+D.



1 Disabled folders shown

2 Disabled folders concealed

More information:

[Concealing Hidden Policy Items](#) (see page 54)

[Disabling a Folder](#) (see page 50)

Enforced Policy Folders and Settings

Enforced items are an ideal method for selectively preventing policy changes. When you enforce an individual setting, it cannot be edited in a child policy. When you enforce an individual folder, all settings in the folder are fixed and cannot be edited in a child policy. Subfolders are not enforced automatically.

Enforcing a Folder or Setting

To enforce individual items

1. In the Policy Editor, select a single folder or setting
2. Click  or right-click and choose Enforced.

To enforce subfolders

In the Policy Editor, right-click a folder and choose Enforce Branch. This has the same effect as enforcing an individual folder, except it applies to all subfolders in the policy branch.

To enforce policy changes in child policies

By default, any change made to a setting in a parent policy is automatically applied but not enforced in a child policy. However, you can enforce these changes in child policies.

In the Policy Editor, choose Tools, Automatically Enforce Modified Settings.

Note: If you enforce a disabled folder , it cannot be re-enabled in a child policy. Equally, if you enforce an enabled folder, it cannot be disabled in a child policy.

To unenforce items

Naturally, you cannot unenforce folders or settings in a child policy. You can only unenforce items by editing the policy in which the attribute was set. In the Policy Editor, to unenforce:

- A single folder, select an enforced folder and click .
- An entire branch, right-click a folder and choose Unenforce Branch

Note: If a folder is enforced, you cannot unenforce individual settings within the folder. Also, you cannot unenforce folders in a child policy if the equivalent folder is enforced in a parent policy.

Enforced Folders and Policy Branch Inheritance

The Enforce attribute is exempt from automatic policy branch inheritance. When you enforce a folder, this only enforces settings within the current folder and within the equivalent folder in any child policies.

- To enforce settings within all subfolders, right-click a folder and choose Enforce Branch.
- To unenforce an entire branch, right-click a folder and choose Unenforce Branch.

Enforcing Modified Settings in Child Policies

By default, any change made to a setting in a parent policy is automatically applied but not enforced in a child policy. This means that the setting can still be modified in the child policy. For example, an administrator can undo an inherited change to an individual user's policy. However, you can optionally enforce these changes in child policies.

For user policy, this means you can enforce changes made to a group policy when they are inherited by users and groups lower down the group hierarchy.

For machine policy, this means you can enforce changes made to the common gateway policy or common client policy when they are inherited by individual gateways or client machines respectively.

To enforce inherited changes in child policies

In the Policy Editor, choose Tools, Automatically Enforce Modified Settings. This menu item has a checkbox:

- By default, this setting is disabled (the checkbox is not selected). Changes made in a parent policy are not enforced in the child policy. Settings in the child policy inherit the new values but are not enforced: 
- If you enable this setting (select the checkbox), then changes made in a parent policy are enforced in the child policy. Settings in the child policy inherit the new values and these settings are now enforced: 

Hidden Policy Folders and Settings

Because the user policy is so extensive, it can be hard to focus on the areas you want to review or edit. To simplify the information displayed in the Policy Editor, you can mark individual folders or settings as hidden. You can then choose to show or conceal these hidden items in the Policy Editor.

Hiding a Folder or Setting

If you hide a folder, its subfolders and settings are also hidden. Likewise, if you hide a folder in a parent policy, the equivalent folder in any child policies is also hidden.

To hide an item

1. In the Policy Editor, select a folder or setting
2. Click . Or right-click and choose Hidden.

Folder and setting icons change to  and  in the Administration Console. You can now choose to show or conceal these hidden items.

To unhide items

Select a hidden item ( or ) and click  again.

Note: You cannot unhide individual settings within a hidden folder. Also, you cannot unhide folders in a child policy if they have inherited this attribute from a parent policy.

More information:

[Policy Inheritance](#) (see page 45)

[Concealing Hidden Policy Items](#) (see page 54)

Concealing Hidden Policy Items

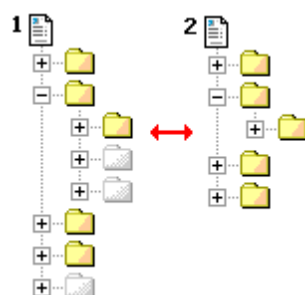
By default, hidden folders and settings are shown in the Policy Editor, but you can conceal these items. That is, you can configure the Policy Editor so it does not display hidden folders or settings.

To conceal hidden items

Choose View, Show Hidden Items to conceal these items. Or press Ctrl+H.

Example: Show hidden items

If hidden items are concealed in the Policy Editor, you can undo this by choosing View, Show Hidden Items. Or press Ctrl+H.



1 Hidden items shown.

2 Hidden items concealed

More information:

[Hiding a Folder or Setting](#) (see page 53)

[Conceal Disabled Folders](#) (see page 51)

Controlling Policy Changes

You need to prevent unauthorized or conflicting changes to user and machine policies. This is especially important if you have multiple administrators (that is, CA DataMinder users with administrative authority). Follow these steps:

1. Decide who is permitted to edit (or even view) policies. You create *policy administrators* by the prudent allocation of administrative privileges.

Policy privileges

Certain administrative privileges permit users to view and edit policies, and to replicate policy changes to client machines. These are:

- Policies: Edit policy
 - Policies: Edit the CMS policy
 - Policies: Replicate changes to clients
 - Policies: View policy
2. Specify which users, groups or machines can be managed by each of your policy administrators. For example, you may want to restrict an administrator's authority to a specific department or office. To do this, make sure an appropriate management group is assigned to each of your policy administrators.

Management group

After assigning the appropriate privileges to your policy administrators, you need to set their management group to control which user policies they can manage. Administrators cannot view or edit user policies that fall outside their management group.

3. Control which settings and folders within those policies your policy administrators are permitted to edit. To do this, you apply the Enforce and Disable attributes.

Disable and Enforce attributes

Any folder and setting can be *enforced*. This means nobody can edit it in a child policy. Similarly in the user policy, any trigger folder can be disabled. This means CA DataMinder ignores all settings in the folder itself and its subfolders. By using combinations of the Enforce and Disable attributes, you can restrict the folders and settings that an administrator can edit in a child policy. For example, to set up an enterprise-wide Web usage advisory, the primary administrator can enforce the Warning Message folder in the user policy (in the Extensions folder) for the top-level 'Users' group. This means nobody can change the message in any child policy throughout the enterprise.

Likewise, the primary administrator may choose to *disable* certain folders in the policy for the top-level 'Users' group, for example, some unused capture triggers. If they also enforce these disabled folders, this ensures that nobody can re-enable these triggers in any child policy throughout the enterprise.

Chapter 5: Editing Policies in the Administration Console

From the Administration console, you can launch the User Policy Editor to edit the policy for any user or group in your CA DataMinder deployment.

This section contains the following topics:

[User Policy Editor](#) (see page 57)

[Edit a Policy](#) (see page 58)

[Find a Policy Folder or Setting](#) (see page 59)

[Policy Reports](#) (see page 60)

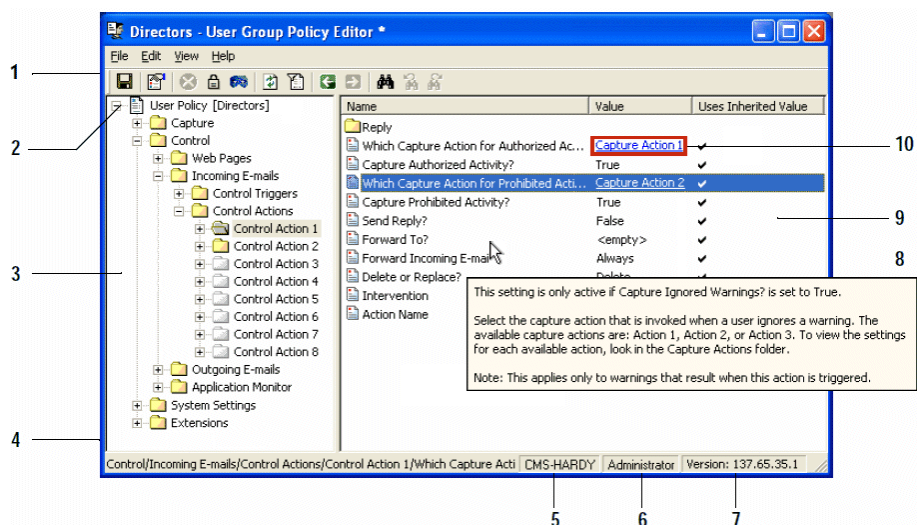
[User Definitions](#) (see page 62)

[Export, Import, and Copy Policies](#) (see page 63)

[Included, Excluded, and Ignored Items](#) (see page 64)

User Policy Editor

The User Policy Editor is where you edit policies for user groups or individual users. These policies govern how users use email, manage their files, print documents, and submit data to web sites.



1. **Toolbar.** Each screen has its own set of tools and features.
2. **Policy root.** This indicates which user or group the current policy applies to.
3. **Policy folders pane.** This shows all the folders available for viewing or editing in the current policy. Icon variations show the folder status (disabled, enforced or hidden).

4. **Policy path.** This shows the location of the current folder or setting within the policy.
5. **CMS.** This is CMS that you are currently logged on to.
6. **User name.** This is the CA DataMinder logon name for the current console user.
7. **Policy version.** Shows the current policy version number. This enables administrators to track policy updates.
8. **Policy explanations.** Hover your mouse pointer over any folder or setting to see a tooltip explanation. Help is also available when you double-click a policy item.
9. **Contents pane.** Shows the settings or subfolders in the current policy folder. Icon variations show the status of each setting or subfolder (disabled, enforced or hidden). You can also double-click a setting to view or edit its value.
10. **Hyperlink.** Many settings are hyperlinked to a dependent setting. Click the hyperlink to jump to the specified setting.

More information:

[Wildcards and Policy List Items](#) (see page 68)

[Policy Version Numbers](#) (see page 47)

[Included, Excluded, and Ignored Items](#) (see page 64)

[Enforcing Modified Settings in Child Policies](#) (see page 53)

Edit a Policy

To edit a policy

1. In the User Administration or Machine Administration screen, select a user, group or machine.
2. Do one of the following:
 - Click Edit Policy 
 - Right-click and choose Edit Policy
- Note:** To view a policy in read-only mode, right-click and choose View Policy.
3. In the Policy Editor screen, browse the policy folders  to find the setting you want.
4. Double-click the setting  to edit its value or attributes.

Important! Click  to save your policy changes.

When you save the updated policy, a summary dialog lists all policy items that you have modified. This dialog allows you to confirm, cancel or modify the changes.

Find a Policy Folder or Setting

To quickly find a specific folder or setting, use the Find feature

1. Open the policy you want in the Administration console.
2. In the Policy Editor screen, click  or press Ctrl+F.
3. Enter the setting or folder name in the Find dialog.

You do not need to enter the whole name. You can search on the first few letters of any word in the name, and you do not need to match the case.

For example, type 'use' to find the first 'Message To Users' setting.

4. You can quickly search the policy tree to find other occurrences of this name:

To find the previous occurrence of this name, click  or press Shift+F3.

To find the next occurrence of this name, click  or press F3.

More information:

[Policy Reports](#) (see page 60)

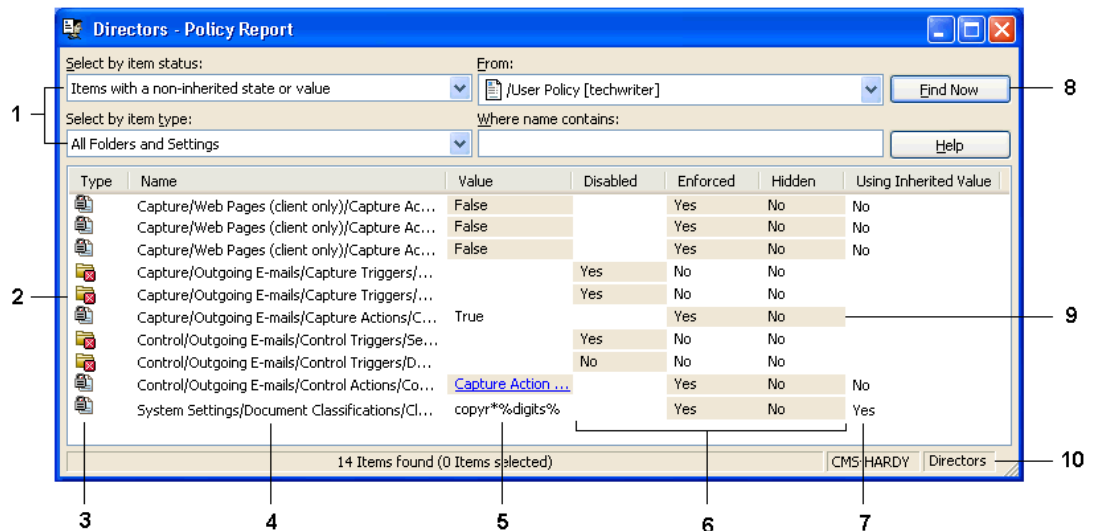
Policy Reports

Editing policies can involve extensive changes to similar-settings. For example, you might want to quickly compare the Search Text words and phrases used by your Data In Motion and email triggers. Or you may want to re-enable various triggers but you cannot remember which ones are explicitly disabled. These are typical problems facing policy administrators, especially where policy editing privileges have been granted to multiple administrators.

Policy reports eliminate these problems and allow you to keep track of changes to individual policies. Policy reports gather the settings or folders that interest you into a single list and let you make instant changes to values and attributes. You can even copy report items into external documents or spreadsheets. This can be useful, for example, if you want to compare settings in different policies.

Policy reports are available for both user and machine policies. The scope of each report is shaped by the report filters. For example, you can quickly identify items that have been edited in the current session or that do not use default (inherited) values or attributes. You can further refine the report to include only particular types of settings (for example, list settings or True/False settings) or policy items with specific names. Finally, you can choose which parts of the policy to report on; you can generate a report for the entire policy, or you can limit it to a specific branch.

For example, if a policy report reveals that your email triggers are using different Search Text values to your Data In Motion triggers, you can immediately edit your email settings without returning to the Policy Editor screen. Likewise, you can run a single report to identify all disabled triggers and instantly re-enable them.



Policy Report dialog

1. **Report filters:** Pinpoint the policy items you want using the report fields: Select, Show, From, and Where name contains.

2. **Report items:** Right-click items to edit values, change attributes, locate or copy.
3. **Type column:** Icons identify settings and folders and also indicate the item status (hidden, enforced or disabled).
4. **Item name:** Shows the full name and policy path of the setting or folder.
5. **Setting value:** Shows the current value of each setting.
6. **Attributes:** Shows the current attribute status (Disabled, Enforced, Hidden) of each setting and folder.
7. **Using Inherited Value:** A 'No' value indicates that the value has been customized and differs from the value that the setting inherited.
8. **Find Now button:** Click to generate a policy report based on the current report filters.
9. **Customized setting or attribute:** Highlights identify items that have been customized. That is, the current value or attribute differs from the inherited value or attribute.

Generate Policy Reports

To generate policy reports

1. Open the policy you want in the Administration console.
2. In the Policy Editor screen, choose the scope of the policy report. To report on:
 - The whole policy,** click  or right-click the policy root  and choose Report.
 - A policy branch,** right-click the policy folder  you want and choose Report. The resulting report only covers items in the current folder and its subfolders.

Note: You can easily change the report scope by re-selecting the 'From' filter. See Step 3.
3. In the Policy Report dialog, select the report filters.
4. Click Find Now to run the report.
5. You can right-click report items to edit their values, change their attributes (Hide, Enforce, or Disable), locate them in the Policy Editor, copy them to the clipboard, or even save them as spreadsheet-compatible files. Choose from the available actions.

Note: To select multiple items, hold down the Ctrl key while clicking with the mouse to select the items you want. For example, you can hide or reset multiple items at one time.

User Definitions

User definitions, also known as 'replaceable strings' are variables that can be referenced by any settings in the current user policy that have a text value (for example, trigger names, address lists, search text lists, messages to users). For example, you can define a 'Disclaimer' user definition and reference this as %Disclaimer% in any Trigger Name setting.

Example

For example, you can add a 'Disclaimer' user definition and set its value to:

Unipraxis distributes this document for informational purposes only.

You can then reference this definition as %Disclaimer% in any other policy trigger. For example, you can include this definition in the explanatory message that users see when their email is blocked, for example:

"Your email has been blocked because it does not include the mandatory corporate disclaimer: %Disclaimer%"

To set up a user definition

1. Open the policy you want in the Administration console.
2. In the Policy Editor screen, browse to the System Settings folder.
3. In the Definitions policy folder, select the User Definitions setting and the User Definition you want to configure.
4. Enter a name for the user definition, such as 'Disclaimer'.

Note: This name is case sensitive and must not contain spaces or a percentage symbol (%).

5. Enter a value for the definition, such as:

Unipraxis distributes this document for informational purposes only.

6. This user definition can now be referenced as a string value in any other policy trigger, for example, in a Message To Users setting:

"Your email attachment has been blocked, as it is missing its mandatory corporate disclaimer: %Disclaimer%"

Notes:

- If you inadvertently define multiple User Definitions with the same name, then any duplicate definitions are ignored and an error is written to the Activity log.
- User definitions can themselves contain variables specified by other user definitions. Ensure that you do not create circular references. For example, if User Definition 1 references User Definition 2, User Definition 2 must not reference User Definition 1.

More information:

[Variables in User Notifications and Email Replies](#) (see page 351)

Export, Import, and Copy Policies

You can use the Policy Editor to export and import policies to and from files, copy a policy from one account to another, and check policy versions. These operations are equally applicable to user policies and machine policies.

This functionality is also available through a command line using wgnpol.exe. For example, you can incorporate policy operations into scripts or batch files. This is installed automatically using the server installation wizard and, for standalone client installations the client installation wizard. For command line details, see the *Platform Deployment Guide*; search for wgnpol.exe.

To export, import or copy a policy

Follow instructions 1-3 and then see the relevant section below.

1. Open the policy you want in the Administration console.
2. In the Policy Editor screen, choose one of the following:
 - File, Export policy
 - File, Import policy
 - File, Copy policy
 - File, Export Policy Blueprint

To export the current policy to an XML file

1. In the Policy Editor screen, choose File, Export.
2. In the Export Policy to File dialog, specify the name and location of the file you want to export the policy to.
3. Complete check box: Select this check box to export the entire set of policy triggers in the selected policy. If you do not select this check box, only the policy settings that have changed from the default settings are exported. This is known as 'sparse' policy.

Note: Exported policies are saved as XML files and can be reimported.

To import a policy from an XML file

1. In the Policy Editor screen, choose File, Import.
2. In the Import Policy to File dialog, locate the source policy file you want to import.

Note: You can only import XML policy files.

3. If you are importing from a 'complete' source policy XML file, you must select the Complete check box. If you do not select this check box, the import will fail.

Note: A 'complete' source policy file is one that contains all policy triggers and not simply those triggers that have changed from the default settings.

You can use wgnpol.exe to import items from a CSV file to a list setting in a user policy.

Note: Policy names correspond to CA DataMinder account names for users, groups or machines.

To export policy as human-readable spreadsheet

1. In the Policy Editor screen, choose File, Export Policy Blueprint.
2. In the Export Policy Blueprint dialog, specify the name and location of the file you want to export the policy to.

Note: Human-readable policy blueprints are saved as XLS files and cannot be re-imported.

To copy a policy from one account to another

1. In the Policy Editor, choose File, Copy Policy To.
2. In the resulting dialog, select the target account. That is, choose where you want to copy the current policy to.

Included, Excluded, and Ignored Items

All triggers in the user policy can use lists of included, excluded, or ignored items. You specify which list is checked for matching items. Examples include lists of matching URLs, file names, email addresses, search text, and so on.

Included lists

Included items are *forbidden* items. If a trigger uses an Included list, any single item in the list can activate the trigger. If a trigger fails to detect any items in the Included list, the trigger does not activate. For example, if a Web page capture trigger uses an Included URL list, any URL on this list triggers a capture when the user browses to it.

Included Addresses lists also affect data lookup commands that use %sender%, %recipient%, %senderalias% or %recipientalias% variables. If a trigger uses an Included list, these data lookup commands only evaluate included email addresses.

Excluded lists

Excluded items are *allowed* items. If a trigger uses an Excluded list, any items can activate the trigger except items in this list. If a trigger fails to detect any items in the Excluded list, the trigger activates.

For example, a control trigger for incoming emails uses an Excluded Addresses list. The trigger always activates when it detects an incoming email unless the email is from a sender on the Excluded list. If it is from an Excluded sender, the trigger does not activate.

Excluded Addresses lists also affect data lookup commands that use %sender%, %recipient%, %senderalias% or %recipientalias% variables. If a trigger uses an Excluded list, these data lookup commands do not evaluate excluded email addresses.

Note: Excluded lists containing multiple items require special attention. For these lists, Web pages, files, or emails are only exempted if all listed items are detected. For example:

- An outgoing email sent to multiple recipients is only exempted if all recipients are on the Excluded Addresses list. If any of the recipients are absent from the Excluded Addresses list, the trigger will activate as normal!
- A Search Text trigger for Web pages that specify multiple excluded words always activates unless every word on the Excluded text list is detected on the Web page. If any listed words are missing, the trigger activates as normal. If all listed words are detected, the trigger does not activate.

Ignored lists

Available only for file and email address lists.

If a trigger has email addresses or top level file names in an Ignored list, these addresses and files are ignored by the trigger and cannot cause the trigger to activate. In effect, ignored item lists enable you to exempt specific files and email addresses from normal control trigger operations.

For example, a control trigger for outgoing emails blocks emails sent between the Research and Sales teams, but the Research manager is exempted from this rule and so added to the Ignored Addresses list. When the trigger detects emails sent by the Research manager to any member of the Sales team, the trigger infers that it must ignore the email and does not activate.

Ignored Addresses lists also affect data lookup commands that use %sender%, %recipient%, %senderalias% or %recipientalias% variables. If a trigger uses an Ignored list, these data lookup commands do not evaluate ignored email addresses.

Note: CA DataMinder disregards the Ignored list if the Included list is set to '*' (the * wildcard equates to 'include everything').

More information:

[Define a Policy List](#) (see page 67)

[Wildcards and Policy List Items](#) (see page 68)

[Combination List Checking](#) (see page 71)

[Multiple Message List Items](#) (see page 71)

[Copy and Import List Items](#) (see page 73)

[Changing the List Source](#) (see page 76)

Define a Policy List

To define a list of trigger items, you edit the associated policy list setting. These settings use a special version of the Policy Setting Properties dialog.

To define a list of trigger items

1. Open the policy you want in the Administration console.
2. In the Policy Editor screen, locate the trigger with the list setting you want to change. Example list settings include Excluded Addresses and Included Search Text.
3. Double-click the list setting or right-click and choose Properties.

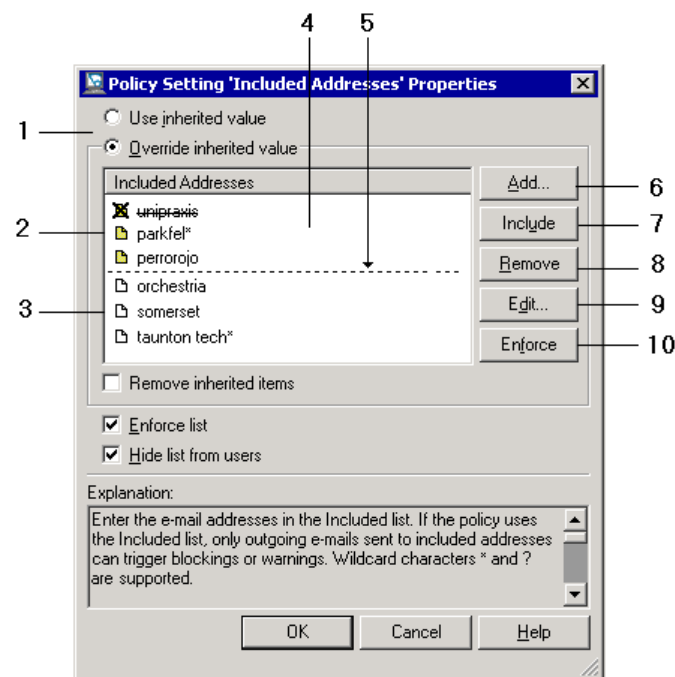
This opens the Properties dialog.

4. Use the Add, Exclude and Remove buttons to define your list.

You cannot add multiple items into a single row of the list box. You must add items to separate rows. For example, you cannot add this as a single entry:

```
file1.txt;file2.txt;file3.txt
```

In lists of email addresses, spaces are interpreted as AND operators.



Policy Setting Properties dialog: example list settings

- 1 List source options: 'Use inherited value' and 'Override inherited value'.
- 2 Default list items, inherited from the parent policy.
- 3 Custom list items, added to the current policy.
- 4 List box. Right-click here to copy, paste or import list items.
- 5 Dashed line. Separates default items from custom items.
- 6 Add button.
- 7 Include or Exclude button. Available only when you select a default item.
- 8 Remove button. Available only when you select a custom item.
- 9 Edit button.
- 10 Enforce button.

More information:

[Spaces in Email Addresses](#) (see page 153)

Wildcards and Policy List Items

CA DataMinder supports the * and ? wildcards in policy list items. You can substitute * for zero or more characters; you can substitute ? for a single character. The following table provides examples:

List items	Notes
URLs	* characters are added are automatically to start and end of these items.
unipraxis	Interpreted to be the same as *unipraxis*. The trigger detects sites such as unipraxis.com, unipraxis.co.uk or even sales.unipraxis.com.
sales.*.com	Detects sites such as sales.unipraxis.com.
Email addresses	Email address matching is not case-sensitive. CA DataMinder interprets a space between address components as AND operators.
*@unipraxis.com	Detects emails sent to or from this domain only.
@unipraxis	Detects emails sent to or from domains such as unipraxis.com or unipraxis.co.uk.
unipraxis.com	Detects any email addresses ending in 'unipraxis.com'. In effect, this is the same as specifying *@unipraxis.com.
frank unipr*	Detects all emails sent to or from, for example, frank.schaeffer@unipraxis.com.

List items	Notes
Card numbers	CA DataMinder ignores spaces so, if you prefer, you can omit spaces between digit groups, for example, 45449?00*.
4544 9?00 *	If part of an Included list, the trigger activates whenever CA DataMinder detects a number such as 454491000000. If part of an Excluded list, the trigger is activated whenever CA DataMinder detects any card number except 454491000000.
Text	Trigger text can apply to the content of a file, Web page, email or email attachment, plus data submitted to a Web site using an HTML form.
unipr* or ref???	If part of an Included list, the trigger activates whenever CA DataMinder detects words such as Unipraxis or ref328.
holiday req*	If part of an Excluded list for an email content trigger, the trigger activates for all emails except those that contain phrases such as 'holiday request'.
photocop*	If part of an Excluded list for a submitted data trigger, the trigger activates for all data submissions except when, for example, a user selects 'Photocopier paper' from a form menu.
File names	These include email attachments, imported files, and files uploaded to a Web site.
plan??? or *.xls	If part of an Included list, the trigger activates whenever CA DataMinder detects a file such as plan_13.xls.
*.jpg	If part of an Excluded list, all uploaded files activate the trigger unless this involves a file such as cute_kittens.jpg. Note: Most triggers that use file lists are activated when a listed file is detected; you can specify any file types in these list settings. But other triggers attempt to search the content of the listed files; for these triggers, only certain file types are supported in the file list.
Window titles	Used in Application Monitoring triggers. Note that * characters are added are automatically to start and end of these items.
Notepad	Interpreted to be the same as *notepad*. If part of an Included list, the trigger activates whenever a Notepad window opens.
.do? - Micro	Detects window titles such as 'planning.doc - Microsoft Word'. If part of an Excluded list, the trigger activates whenever a window opens unless it has a title such as 'planning.doc - Microsoft Word'.
Executable paths	Used in Application Monitoring triggers. Note that * characters are added are automatically to start and end of these items.
Notepad	Interpreted to be the same as *notepad*. If part of an Included list, the trigger activates whenever Notepad.exe runs.

List items	Notes
?:*\Foo	This detects any instance of Foo.exe running in a subfolder. If part of an Excluded list, the trigger activates whenever any application runs except for, for example, C:\Program Files\Foo.exe. Note: This does not detect instances of Foo.exe running in the root of a drive, for example, H:\Foo.exe.
Special characters	To search for literal occurrences of the characters { } * or ?, prefix them with a '\' backslash. For example:
24*7	This detects 24*7.
What next for Unipraxis\?	This detects What next for Unipraxis?

Note: CA DataMinder interprets a space between keywords as a literal character except in email address and credit card number lists.

Combination List Checking

Available only for URL and email address lists.

In effect, combination list checking enables you to appoint a censor. For example, combination list checking allows you to block emails sent between the Research and Sales departments unless a copy has also been sent to a particular manager (for example, your regulatory compliance officer).

How does this work? First, the detected URL or address is compared against the Included list. If a match is confirmed, the URL or address is then compared against the Excluded list. If it also appears in the Excluded list, the URL or address is exempted and the trigger does not activate.

To illustrate the required policy settings in the earlier example, the group policy for the Sales department could include a control trigger for outgoing emails with the following list settings:

Which Address List?

This setting is set to:

Use Included list, but exempt if recipient in Excluded list

Included Addresses

This list setting includes:

research.unipraxis.com

Excluded list

This list setting includes:

compliance.officer@unipraxis.com

With these settings, the trigger normally fires if CA DataMinder detects an email sent to frankschaeffer@research.unipraxis.com. But it does not fire if the To: or Cc: lists *also* include compliance.officer@unipraxis.com.

Multiple Message List Items

Some triggers allow you to define separate messages for each item in a list of key words or phrases. When CA DataMinder detects that word or phrase, it displays the corresponding message. This allows you to tailor the message to give the user as much detail as possible, using a single control trigger. For example, you can configure a single trigger to generate the following warnings:

Key text	Example warning if key text is detected
Company X	This email has been blocked. Corporate guidelines do not permit you to send emails to Company X.

Company Y	This email has been blocked. Corporate guidelines do not permit you to send emails to Company Y.
Company Z	This email has been blocked. Corporate guidelines do not permit you to send emails to Company Z.

More information:

[Which Triggers?](#) (see page 72)

[Key Text Separators](#) (see page 72)

[Copy and Import List Items](#) (see page 73)

[Key Text Separators](#) (see page 72)

Which Triggers?

Multiple messages are available for the Included Search Text settings in the following control triggers:

- **Search Text:** Detect the text of incoming and outgoing emails and attachments.
- **Attachments:** Detect the content of incoming and outgoing email attachments.
- **Submitted Search Text:** Detect text submitted to a Web page.

Note: For each trigger, multiple messages are supported only for the Included list of search text. You cannot define multiple messages for Excluded words and phrases.

Key Text Separators

You can associate multiple words or phrases with individual messages, using the | { } characters as list separators. The | character is an OR operator and { } brackets let you define sub-expressions:

Key text	Trigger activates when
recruitment {job offer}	CA DataMinder detects either 'recruitment' or 'job offer'.
sales {forecast projection}	CA DataMinder detects either 'sales forecast' or 'sales projection'.
Company {X Y Z}	CA DataMinder detects 'Company X', 'Company Y' or 'Company Z'.

More information:

[Multiple Message List Items](#) (see page 71)

Copy and Import List Items

When defining your policy list settings, you can copy items from other list settings or external documents. You can import items from external applications or files. For example, you can quickly copy lists of email addresses, file names, Web sites, or key words and phrases to other settings within a policy or even to other policies.

To copy list items from one policy list setting to another

1. In the Policy Editor screen, right-click the list setting with the items you want to copy and choose Properties.
2. In the resulting dialog, select the items that you want to copy, then right-click and choose Copy.

To select multiple items, hold down the Ctrl key and left-click the items you want.

3. Right-click the target list setting and choose Properties.
4. Right-click the list box choose Paste.

To copy list items from an external application

You can import lists directly from an external application. For example, you can import from an Excel spreadsheet or an OpenOffice text document.

1. In the external application, select and copy the items you want.
2. In the User Policy screen, right-click the target list setting and choose Properties.
3. Right-click the list box choose Paste.

To import list items from a text file

You can import lists from any text file that uses appropriate list separators (commas, semicolons, tabs and new lines).

1. In the Policy Editor screen, right-click the target list setting and choose Properties.
2. Right-click the list box and choose Import.
3. Select the file you want to import from.

To copy URL lists directly from your Favorites folder

1. Open your Favorites folder and view the Properties of any Web site shortcut. You can then copy the URL directly to the Clipboard.
2. In the User Policy Editor, right-click the target list setting and choose Properties.
3. Right-click the list box choose Paste.

To copy addresses directly from an e-mail message

1. Open an e-mail and copy the addresses from the To: Cc: Bcc: or From: fields.
2. In the User Policy Editor, right-click the target list setting and choose Properties.
3. Right-click the list box choose Paste.

To import address lists from Microsoft Outlook

You must first export your Outlook address book to a CSV file and then import the CSV file into a list setting.

1. Run the Import and Export Wizard to export a Contacts folder to a CSV file.
Use the Map Custom Fields feature to remove unwanted data fields. See the Outlook help for details.
The wizard encloses each CSV value in double-quotes.
2. Remove these quotes before you import the CSV file into the list setting.
3. In the User Policy Editor, right-click the target list setting and choose Properties.
4. Right-click the list box choose Import.
5. Select the CSV file you want to import.

To import address lists from Lotus Notes

You must first export your Notes address book to a text file and then import the text file into a list setting.

1. In Notes, open the address book and select the contacts you want to export.
2. Run the Export feature to export the contact details to a text file.
The resulting text file includes all the available details for each contact. But you only need the e-mail addresses, so you must delete all the other details before importing the file into a list setting.
Note: The file may require extensive editing in order to remove all unwanted data. If you are only importing a small number of contacts, this may not be a practical solution.
3. In the User Policy screen, right-click the target list setting and choose Properties.
4. Right-click the list box choose Import.
5. Select the text file you want to import.

More information:

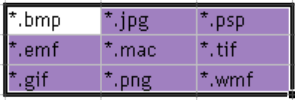
[Supported List Formats](#) (see page 75)

[Commas and Semicolons in Policy Lists](#) (see page 75)

Supported List Formats

You can copy and paste delimited lists from any text editor or text file. CA DataMinder recognizes commas, tabs, semicolons, and line breaks as following separators between items:

You can also copy items from a table or spreadsheet. Copy the items you want to the Clipboard then paste them directly into the target policy list. Below are some examples that can be pasted directly into a list setting:

Formats	Example
Comma*	*.bmp,*.gif,*.jpg,*.png *.bmp, *.gif, *.jpg, *.png
Semi-colon*	*.bmp;*.gif;*.jpg;*.png *.bmp; *.gif; *.jpg; *.png
Tab	*.bmp *.gif *.jpg *.png
New line	*.bmp *.gif *.jpg *.png
Spreadsheet or word processor table	

More information:

[Copy and Import List Items](#) (see page 73)

Commas and Semicolons in Policy Lists

Commas and semi-colons are recognized by CA DataMinder as list separators. If you import or paste list items that contain a literal comma or semicolon, replace the comma or semicolon with \, or \; instead. For example, change this:

"Do not disclose the content or take, retain or redistribute copies of this email."

To this:

"Do not disclose the content or take\, retain or redistribute copies of this email."

Changing the List Source

A list setting can include both inherited default items and custom items added by the current user. But you can edit the list properties to only include items from one of these sources. The following actions are available in the Policy Setting Properties dialog for list settings:

Revert to the inherited list

If you want to revert the list back its original state, containing only those items inherited from the parent policy, select the Use inherited value option. This removes all custom list items and undoes any excluded default list items.

Remove all inherited list items

If you want the list to only include custom items, select the Remove inherited items check box. This removes all list items inherited from the parent policy.

Chapter 6: Editing Policies in the iConsole

Use the iConsole Policy tab to edit the CA DataMinder standard policies.

Note: The Policy tab is only available in the iConsole if you have installed a CA DataMinder policy pack on your CMS and iConsole servers.

This section contains the following topics:

[Available Policies](#) (see page 77)

[Available Actions](#) (see page 94)

[Who Do the Standard Policies Apply To?](#) (see page 98)

[FPP User Groups Created Automatically on the CMS](#) (see page 98)

[Editing Policy in the iConsole](#) (see page 100)

[Policy Tuning](#) (see page 105)

Available Policies

The iConsole standard policies comprise a predefined set of policies. You can customize these standard policies in the iConsole to quickly roll out CA DataMinder across your organization.

Standard policies are organized into classes, such as 'Corporate and Regulatory Compliance' and 'Personally Identifiable Information (PII)'. Each policy class contains several individual policies. For example, the PII policies include 'Account Number' and 'Credit Card Information' policies.

Individual policies are based on triggers in the user policy, plus other key settings such as document classifications. However, you must edit these standard policies in the iConsole.

The following sections provide summary descriptions of the CA DataMinder standard policies.

Note: The following sections do not necessarily list the complete set of policies. For example, the available policies may vary according to your CA DataMinder license. Use the iConsole to view the complete set of policies available to your organization.

More information:

[Corporate and Regulatory Compliance Policies](#) (see page 78)

[Customer / Supplier Treatment Policies](#) (see page 80)

[Employee Behavior Policies](#) (see page 81)

[Intellectual Property \(IP\) Policies](#) (see page 82)

[Legal Policies](#) (see page 83)

[Non-Public Information \(NPI\) Policies](#) (see page 84)

[Personal Health Information \(PHI\) Policies](#) (see page 86)

[Personally Identifiable Information \(PII\) Policies](#) (see page 86)

[Security General / Corporate Policies](#) (see page 90)

[User Defined Policies](#) (see page 93)

Corporate and Regulatory Compliance Policies

Anti-Money Laundering - OFAC

This policy detects suspicious financial transactions such as tax evasion or false accounting, especially with entities that appear on the U.S. OFAC list.

Bid Rigging Detection: Insurance

This policy identifies 'B' bids, and other electronic communications indicative of bid rigging, as it relates to the insurance industry.

Bid Rigging Detection: Municipal Bond Issuance

This policy detects language that indicates possible bid rigging related to Municipal Bond issuance.

Blast E-Mail

This policy monitors for blast e-mail which is sent to more than a specified number of external recipients at one time.

Bribes/Kickbacks/Quid Pro Quos/Blackmail

This policy detects involvement in bribery or blackmail schemes.

Broker Error

This policy detects indications that a broker has made or is attempting to correct an error with respect to trading.

Communication with Regulatory, Legal, and Governmental Authorities

Protect and control communications between an employee and regulatory, legal, and governmental authorities.

Fair and Balanced Advice

This policy detects unbalanced communication by recognizing claims and statements that focus solely on positive or negative aspects of a product, advice, or decision.

Information Destruction Alert

Electronic information can be eliminated as easily as it is created, making the uncontrolled destruction of retained information an unacceptable risk. This policy detects text indicative of a suggestion to eliminate e-mail messages, computer files, or documents. It also detects general references to retention rules.

Investment Advice Prohibition

This policy detects messages that appear to contain investment advice or recommendations.

Securities Parking

This policy is designed to look for evidence of two parties engaged in a possible "trade parking", or "wash trade", arrangement.

Solicitations: Charitable

This policy detects solicitations or requests for contributions to charities, student fundraisers, or other non-commercial and non-political organizations.

Solicitations: General

This policy detects language containing general references to contributions or solicitations for contributions.

Solicitations: Political

This policy detects solicitations or requests for contributions to political causes or campaigns.

Solicitations: Private Investments

This policy detects language containing references to contributions or solicitations for contributions to private investment activities.

Solicitations: Religious

This policy detects solicitations or requests for contributions to religious organizations.

Tax Advice Prohibition

In general, a Representative must be both qualified, and allowed by the firm, in order to offer 'advice' to a customer. This policy is designed to identify messages where a non-tax Professional offers tax advice to a public customer.

Trading in an Outside Account: Order Confirmations

This policy detects order confirmations so as to identify trading activity, for one's personal account, outside of firm-approved processes and/or procedures.

Trading in an Outside Account: Order Placements

This policy is designed to identify trade order placements, for one's personal account, outside of Firm-approved processes and/or procedures.

Whistleblower

This policy detects possible whistle blower situations and allows an organization to take appropriate steps in response.

Customer / Supplier Treatment Policies

Customer Complaints: Response Prohibition

Most companies do not allow their representatives to directly respond to a customer complaint. This policy analyzes outbound external e-mail for indications that a representative has directly responded to a customer complaint, which may or may not have been received initially by e-mail.

Customer Complaints: Unprofessional Responses

This policy analyzes outbound external e-mail for indications that a company representative has directly responded to a customer

complaint, which may or may not have been received initially by e-mail, in an unprofessional and/or un-empathetic manner.

Customer Conditioning

This policy detects communications to a customer that include pressuring language. This may include attempts to force the customer to accept products or services they do not want or need.

Customer Threats

This policy detects language that indicates pressure being used against a customer in order to limit business with competitors. This is an example of anticompetitive behavior and can be a violation of anti-trust regulations.

Exclusivity

This policy detects language that suggests an attempt to establish full control over sales to a third party. This is an example of anticompetitive behavior and can be a violation of anti-trust regulations.

Gifts and Entertainment

Gifts and entertainment form a common part of many business relationships, yet have the potential to create conflicts. This policy identifies when a business expense violates policy or law and becomes a gift.

Guarantees and Assurances

Guarantees, though often considered a part of "fair and balanced" communication, carry with them legal, regulatory, and financial risks, as well as risks to a firm's reputation. This policy detects prohibited guarantees or assurances and can be used to prevent them from reaching customers.

Unqualified Rebates or Benefits

This policy is designed to detect an offer of a rebate when the terms and conditions have not been met. This can be used as a method to offer money to a customer for excluding competitors or accepting otherwise unwanted products.

Employee Behavior Policies

Coercive Behavior and Intimidation

Coercive behavior and intimidation in the workplace can have significant negative impact on employee morale and productivity. This policy detects such behavior so that enforcement is confidential and immediate.

Communication with Competitors

This policy detects electronic communication between an employee and competitor companies.

Communication with the Press/News Organizations

This policy detects electronic communication between an employee and the press or media organizations.

Corporate Criticism

This policy detects criticisms and negative comments about the company, its products, or the management team.

Deceptive Language

This policy detects communications that may include false or misleading information. In addition, it will detect references that indicate inappropriate offline communications.

Discrimination and Racism

This policy detects inappropriate discriminatory language and/or actions based on race, gender, disability, sexual orientation, religion, age, and other legally protected classes. Sexual harassment related issues are covered by the Harassment policy.

Discrimination: Age

This policy attempts to identify communications containing words and phrases that indicate a likelihood that age discrimination is taking place or being referenced.

Fantasy Leagues

This policy identifies events and activities associated with participation in or running a fantasy sports league.

Gambling Prohibition

This policy detects gambling and betting among employees which is subject to various jurisdictional regulations. Fantasy leagues are covered by a separate policy.

Harassment

This policy detects harassment such as quid pro quo requests for sexual contact, or behavior that is designed to alarm or annoy others.

Inappropriate, Offensive and Sexual Language

This policy identifies communications indicative of offensive and sexual language.

Intent to Resign

This policy detects language indicative of an employee who is dissatisfied with their position or workplace and is actively engaged in seeking employment.

Jokes

This policy detects electronic communication of a wide range of joke formats and subjects. It does not address communication that originated outside the firm, but will capture such events if the recipient within the firm attempts to forward them.

Office Relationships: Romantic

This policy detects events of a romantic nature, or language indicating that such a personal relationship exists.

Outside Business Activity/Directorships/Employment

This policy identifies communications that suggests an employee is engaged in external business activities unrelated to the company; serving or considering serving on another company's board of directors; or is participating in other activities that might affect the employee's performance at the company.

Termination/Layoff Discussions

Protect communications concerning potential and pending terminations and layoffs.

UK Resumes/CVs

This policy is designed to detect UK resumes in standard format.

US Resumes/CVs

This policy is designed to detect US resumes in standard format.

Intellectual Property (IP) Policies

Confidential Trade Data

This policy detects confidential information such as trade secrets, proprietary processes and technical competitive differentiators.

Patent Applications

This policy detects non public patent applications.

Product and Design Specifications

This policy detects functional or marketing specifications of material, products, or services.

Proprietary Software Code

This policy detects software code, programs, and executables.

Technical Specifications or Designs

This policy detects technical designs and specification documents related to products or services.

Legal Policies

Attorney Client Privilege

When an uncontrolled privileged communication or document leaves an organization, any privilege associated with it may be waived. This policy prohibits such communication from being sent externally.

Discussion of Legal Proceedings

This policy detects events related to legal proceedings such as pending civil lawsuits, criminal proceedings, and/or administrative hearings or trials. Threats of contemplated litigation against the organization are not intended to be covered by this policy.

Potential Ethical Issues

This policy identifies potential ethical misconduct or claims of ethical misconduct and alerts the proper internal legal representative.

Potential Legal Issues

Often, questions are circulated internally about the legality of a particular action or business practice without informing a legal representative until the problem has been made public or resulted in some harm. This policy identifies such discussions and alerts the appropriate legal representative.

Threats of Litigation

This policy detects discussions indicating an outside party or an internal employee suggesting or overtly threatening to file a lawsuit against the company.

Non-Public Information (NPI) Policies

Board Minutes and Discussions

This policy is designed to detect events occurring between or concerning board members of an organization.

Corporate Contracts

This policy detects the language that is typically used in corporate contracts.

Customer Lists

This policy detects multiple occurrences of various types of customer contact information.

Draft Documentation

This policy can be used to prevent draft documentation, and discussions surrounding it, being sent outside an organization.

Financial Information - Balance Sheet

This policy detects content found on financial balance sheets.

Financial Information - Income Statement

This policy detects content found on financial income statements.

Financial Information - Projections

This policy detects the disclosure of financial projections.

Information Security Label Control

This policy detects sensitive material classified in various ways such as "confidential", "top secret", and "not for distribution".

Inside Information: Front Running/Trading Ahead

This policy detects messages exhibiting evidence that a market participant is attempting to profit financially by placing transactions before (in front of) another market player, or customer, by leveraging the information a "tipper" possesses about what that market player/customer intends to do.

Inside Information: Non-Public Company Information Loss

Protect and control non-public company insider information, such as management discussions.

Inside Information: Non-Public Financial Information Loss

This policy detects unauthorized disclosure of non-public company financial and stock information.

Inside Information: Rumors and Secrets

This policy detects unsubstantiated information or rumors about any organization or client for legal purposes.

Inside Information: Trading Ahead of Research

Disseminating and acting on non-public, inside information is illegal. The content of a research report may influence the price of the security being discussed. Parties may profit from this non-public information by placing trades ahead of the issuance of the research report. This policy is intended to detect language indicative of two or more parties disseminating non-public information regarding advance knowledge of pending research.

Internal Investigations

This policy detects the existence, purpose, and/or results of company specific investigative matters.

Internal IT Support Documents

This policy identifies internal IT system and support documentation.

Licensing Agreements

This policy is designed to detect information containing software license agreements.

Mergers and Acquisitions

This policy identifies discussions and documents pertaining to pending or proposed merger and acquisition transactions in which the organization is or will be participating. Transactions such as IPOs, private placements, and other prospectus offerings are not expressly included in this policy.

Pricing List

This policy is designed to detect nonpublic pricing information.

Project Information

This policy identifies various types of project information such as project plans, timelines, project codes, task lists, and issue lists related to project planning and deployments.

Restricted List

This policy detects items and content on restricted lists in e-mails and files. Restricted/Watch/Grey Lists are associated with services, products, companies, customers, or other defined business elements that have restrictions.

Sales Information

This policy detects company sales information, sales collateral such as tools, models, contracts, fee structures, and deal information, and other elements supporting the sales organization.

Personal Health Information (PHI) Policies

Benefits Enrollment Information

This policy detects benefit applications and other forms that include personal health information.

Diagnosis Information

This policy detects medical diagnosis information including mental, physical and addiction-related ailments.

Individually Identifiable Health Information (IIHI)

This policy detects individually identifiable information in conjunction with medical information related to patients, employees, or customers.

Medical Billings and Claims

This policy detects medical billing information and claims data including submissions to insurance companies, approvals and denials of payment, and continuing correspondence.

Medical History

This policy detects medical history information including diagnosis and prescription details.

Medical Record Numbers

This policy detects medical record numbers used in the identification and treatment of patients.

Medical Record Numbers - Threshold

This policy detects a specified amount (or threshold) of medical record numbers used in the identification and treatment of patients.

Personally Identifiable Information (PII) Policies

Account Number

This policy detects specific account numbers and/or account numbers that fall within a particular range. Numbers may be entered exactly or matched with a template.

Account Number - Threshold

This policy protects and controls a specified amount (or threshold) of specific account numbers and/or account numbers that fall within a particular range.

Account Number and Routing Information

This policy detects both an organization's account number(s) and the associated routing number(s).

Account Number with Additional PII

This policy detects specific account numbers and/or account numbers that fall within a particular range when accompanied by at least one or more pieces of identifying information such as name, address or DOB that could be used for identity theft.

Australian Medicare Card Number

This policy detects one or more Australian Medicare Card Numbers in various formats.

Australian State Drivers License

This policy detects one or more Australian State Drivers License Numbers in various formats.

Australian Tax File Number

This policy detects one or more Australian Tax File Numbers in standard format.

Background Checks

This policy detects background information checks, including private and often sensitive data that might be communicated inappropriately.

Canadian Social Insurance Number

This policy detects one or more Canadian Social Insurance Numbers in various formats.

Canadian Social Insurance Number - Threshold

This policy detects a specified amount (or threshold) of Canadian Social Insurance Numbers in various formats.

Canadian Social Insurance Number with Additional PII

This policy detects one or more Canadian Social Insurance Numbers when accompanied by at least two pieces of identifying information such as name, address or DOB which could be used for identity theft.

Chinese Identity Card Number

This policy detects one or more Chinese Identity Card Numbers in standard format.

Credit Card Information

This policy detects credit card numbers in various ranges and formats.

Credit Card Information - Threshold

This policy detects a specified amount (or threshold) of credit card numbers in various ranges and formats.

Credit Report

This policy detects inappropriate distribution of credit reports or credit related data issued by consumer reporting agencies (CRAs).

Employee Evaluation Information

This policy is designed to identify employee evaluations, often regarded as private between an employee and an organization.

German Social Insurance Number

This policy detects one or more German National Pension Numbers in standard format.

Hong Kong Identity Card Number

This policy detects one or more Hong Kong Identity Card Numbers in standard format.

Indian Permanent Account Number

This policy detects one or more Indian Permanent Account Numbers in standard format.

Indonesian Identity Card Number (Nomor Induk Kependudukan)

This policy detects one or more Indonesian Identity Card Numbers in various formats.

Irish Personal Public Service Number

This policy detects one or more Irish Personal Public Service Numbers in standard format.

Italian National Identification Number

This policy detects one or more Italian National Identification Number in standard format.

Macau Non-Permanent Resident Identity Card (BIRNP)

This policy detects one or more Macau Non-Permanent Resident ID Numbers in standard format.

Macau Permanent Resident Identity Card (BIRP)

This policy detects one or more Macau Permanent Resident ID Numbers in standard format.

Malaysian National Registration Identification Card Number

This policy detects one or more Malaysian National Registration Numbers in standard format

Pakistan National Identity Card Number

This policy detects one or more Pakistan National Identity Card Numbers in standard format

Singapore National Registration Identity Card

This policy detects one or more Singapore National Registration Identity Card Numbers in standard format

Social Security Number

This policy detects one or more US Social Security Numbers in various formats.

Social Security Number - Threshold

This policy detects a specified amount (or threshold) of US Social Security Numbers in various formats.

Social Security Number with Additional PII

This policy detects one or more US Social Security Numbers when accompanied by at least one or more pieces of identifying information such as name, address or DOB that could be used for identity theft.

Taiwan Identity Card Number

This policy detects one or more Taiwan Identity Card Numbers in standard format.

Thailand Population Identification Code

This policy detects one or more Thailand Population Identification Codes in standard format.

UK Drivers License

This policy detects one or more UK Driving License Numbers in various formats.

UK Drivers License - Threshold

This policy detects a specified amount (or threshold) of UK Driving License Numbers.

UK Employee Compensation Information

Protect and control information related to the compensation of their UK employees to identity outside the organization, to a particular group (such as HR), or to a select circle of individuals that are allowed to receive and send such compensation information.

UK National Insurance Number

This policy detects one or more UK National Insurance numbers (the U.K. equivalent of the U.S. SSN), in various formats.

UK National Insurance Number - Threshold

This policy detects a specified amount (or threshold) of UK National Insurance Numbers in various formats.

UK National Insurance Number with Additional PII

This policy detects one or more UK National Insurance Numbers when accompanied by at least two pieces of additional identity information such as name, address or DOB that could be used for identity theft.

UK Tax Identification Number

This policy detects one or more UK Tax Identification Numbers in various formats.

UK Tax Identification Number - Threshold

This policy detects a specified amount (or threshold) of UK Tax Identification Numbers in various formats.

Unencrypted Wire Transfer Information

This policy assists organizations that want to be alerted to or prevent unencrypted disclosure of wire transfer information.

US Drivers License

This policy detects one or more US Drivers License Numbers in various formats.

US Drivers License - Threshold

This policy detects a specified amount (or threshold) of US Driver License Numbers in various formats.

US Employee Compensation Information

This policy detects information related to compensation for US employees being disclosed to parties outside the organization.

US Passport Number

This policy detects US Passport Numbers in various formats.

US Passport Number - Threshold

This policy detects specified amount (or threshold) of US Passport Numbers in various formats.

US Taxpayer Identification Number (TIN)

This policy detects US Taxpayer Identification Numbers in various formats.

US Taxpayer Identification Number (TIN) - Threshold

This policy detects a specified amount (or threshold) of US Taxpayer Identification Numbers in various formats.

Vietnam ID Card Number

This policy detects one or more Vietnam ID Card Numbers in standard format.

Security General / Corporate Policies

Audio Files

Sensitive information may be recorded and sent out of the organization. Protect and control the transmittal of audio media files.

E-mail to Personal Addresses

This policy identifies electronic communication with attachment(s) being sent to non-commercial domains (Hotmail, Yahoo, Gmail, and domains ending in .gov, .edu, .info, and so on), which immediately raises concerns as to whom the information is being distributed.

Forwarding Senior Management E-mail or Documents

This policy detects the forwarding of content originally sent by senior management.

Graphic and Image Files

This policy identifies graphic and image files in various formats.

Large Message or File Size

This policy identifies users sending messages over a certain size or files over a certain size.

Large Print Job Warning

This policy detects print jobs that exceed a specified number of pages and warns the user.

Network Security Threats

This policy identifies common hacking utilities and terms such as spoofing, buffer overflow tools, log wiping tools and password database cracking tools.

Password Protection/Encryption: Prohibition

This policy detects content that has been protected with a password or has been encrypted.

Random Sample

Regulators suggest that adding a targeting a reasonable percentage of messages for random review, in addition to normal lexicon-based reviews, is a prudent practice since such random reviews may discover issues not normally detected by ordinary means. This policy will randomly select messages, based on a percentage that is defined by the firm, to be automatically included in a reviewer's queue.

Sharing of Usernames and Passwords

This policy detects the disclosure and sharing of passwords both inside and outside the organization.

Suspicious E-mail Behavior

This policy identifies electronic communication with blank subjects whose context suggests that the sender is attempting to avoid detection.

Transfer of Attachments - Threshold

This policy identifies electronic communication with a specified number (or threshold) of attachments, which could suggest a drive dump or other inappropriate bulk transfer of files.

Transfer of Personal E-mail File Folders

This policy identifies inappropriate bulk transfer of e-mail file folders which includes .PST and .NSF files.

Video Files

This policy identifies video media files in various formats.

User Defined Policies

By default, these policies are empty. They allow you to define your own policy criteria. You can use them to test your CA DataMinder setup. They also enable you to define your own custom policies if you have a particular requirement that is not fulfilled by the policy pack.

Common Content

For each user-defined policy, you can define the key text that you want CA DataMinder to detect.

Immediate Disqualifiers

Immediate Disqualifiers are words or phrases which immediately result in a non-match if CA DataMinder detects them in an email, file, or web page. That is, the email, file, or web page definitely does not match the policy criteria. CA DataMinder does not apply policy to these items even if they contain other sensitive words or phrases.

Note: A single word or phrase is sufficient to prevent CA DataMinder from applying policy.

Positive Indicators

Positive Indicators are preferred words or phrases. If CA DataMinder detects these words or phrases in an email, file, or web page, it increases the probability that the item matches the policy criteria.

A single Positive Indicator word or phrase is sufficient to trigger policy if no other excluding criteria are detected (such as excluded file names or URLs).

User Defined 1

This policy detects the key words and phrases that you specify in the Common Content settings.

You can define the severity, the policy action, and the resulting message that is seen by users. For the CA DataMinder Enterprise Edition, you can also assign smart tags to classify any captured items.

- For email policies, you can specify excluded search text (CA DataMinder ignores emails containing these words or phrases). You can also specify **included** sender addresses (CA DataMinder only applies this policy to emails from these senders).
- For Files In Motion and Data At Rest policies, you can specify excluded file names (CA DataMinder ignores these files) and a minimum file size (CA DataMinder ignores any smaller files).
- For Web policies, you can specify excluded URLs (CA DataMinder does not apply policy to these web pages).

User Defined 2

This policy detects a second set of key words and phrases. It provides the same settings as the *User Defined 1* policy, with one difference for email policies.

For email policies, you can specify **excluded** sender addresses (CA DataMinder ignore emails from these senders).

User Defined 3

This policy detects a third set of key words and phrases. It provides the same settings as the *User Defined 1* policy, with one difference for email policies.

For email policies, you can specify **excluded** sender addresses (CA DataMinder ignore emails from these senders).

Available Actions

The following policy actions are available in the iConsole.

Available Actions: Email

Email actions refer user activity detected by CA DataMinder email server agents and email endpoint agents. These actions let you block specified emails, or simply warn the sender. You can also encrypt unencrypted outgoing emails or simply monitor and capture email traffic. The available actions are:

Monitor

A copy of the email is captured and stored on the CMS. No other action is taken.

Advise Encryption

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog to the email sender. The sender can choose one of the following:

Encrypt

CA DataMinder inserts an 'encryption request' x-header into the email. This x-header is subsequently detected by a third-party encryption provider, which in turn encrypts the email before it leaves your network.

Don't Encrypt

The email is sent unencrypted.

Cancel

The email is not sent.

For emails detected by a CA DataMinder email server agent:

- If server-side interactive warnings are **not** enabled, CA DataMinder does not intervene and the email is sent **unencrypted**.
- If server-side interactive warnings **are** enabled, CA DataMinder sends a warning email to the sender. If the sender replies to the warning promptly, their original email is released and sent **unencrypted** to its intended recipients. If they do not reply (or reply too late), their original email is disposed of without being sent.

Important! If server-side interactive warnings are enabled, make sure that the message to users in the warning email clearly explains the consequences of replying and not replying! In particular, note the different reply handling for the Advise Encryption and Enforce Encryption options.

Enforce Encryption

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog, as above. But this time, the sender can only choose to Encrypt their email or they can Cancel it. They cannot send an unencrypted email.

For emails detected by a CA DataMinder email server agent:

- If server-side interactive warnings are **not** enabled, CA DataMinder automatically encrypts the email before sending it.
- If server-side interactive warnings **are** enabled, CA DataMinder sends a warning email to the sender. If the sender replies to the warning promptly, their original email is released and sent **encrypted** to its intended recipients. If they do not reply (or reply too late), their original email is disposed of without being sent.

Important! If server-side interactive warnings are enabled, make sure that the message to users in the warning email clearly explains the consequences of replying and not replying! In particular, note the different reply handling for the Advise Encryption and Enforce Encryption options.

Warn

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog. You can configure the warning message. The warning dialog lets the sender choose whether to continue or not.

For emails detected by a CA DataMinder email server agent, the handling is different:

- If server-side interactive warnings are **not** enabled, CA DataMinder automatically sends the email without displaying a warning.
- If server-side interactive warnings **are** enabled, CA DataMinder sends a warning email to the sender. If the sender replies to the warning promptly, their original email is released and sent to its intended recipients. If they do not reply (or reply too late), CA DataMinder deems that they have heeded the warning and their original email is disposed of without being sent.

Note: Warn actions are not supported for emails detected by CA DataMinder Network.

Block

CA DataMinder blocks the email and displays the Block dialog. Use the dialog notification message to explain to the sender why this action was taken.

Note: The Blocking dialog is not shown for emails detected by CA DataMinder Network. The exact handling varies according to the Webmail application. For example, the blocking may be silent, or the user may see a message such as 'We can't connect to Windows Live Hotmail right now.'

Global Option

You can also specify a 'Forward To' email address for each of the above actions. When the action is invoked, CA DataMinder forwards a copy of the email to the specified address.

Available Actions: Files In Motion

Files In Motion actions let you control files being moved across a network, copied to a removable device or writable CD drive, or sent to a printer. These actions also control files entering or leaving the corporate network. In all cases, you can block the files, show a warning to the user, or simply capture the file attributes. For files being copied to removable devices or network locations, you can also encrypt unencrypted files. The available actions are:

Monitor

CA DataMinder captures the file and stores it on the CMS. No other action is taken.

Advise Encryption

CA DataMinder displays a warning dialog. The user copying the file can choose one of the following:

Encrypt

CA DataMinder prompts the user for a password, and uses this password to encrypt the file on the removable device.

Don't Encrypt

The file is copied onto the removable device unencrypted.

Cancel

The file is not copied.

Note: CA DataMinder cannot encrypt files being copied to network locations. Do not use Advise Encryption or Enforce Encryption control actions to prevent unencrypted files being copied to shared locations on your network.

Enforce Encryption

CA DataMinder displays a warning dialog, as above. But this time, the user can either encrypt their file or they can cancel the copy operation. They cannot copy an unencrypted file.

Warn

CA DataMinder displays the Warning dialog. You can specify customized warning messages for each policy. The warning dialog lets the user choose whether to continue or not.

Note: Warnings are not supported for files detected by CA DataMinder Network.

Block

CA DataMinder blocks the print job or copy operation and displays the Blocking dialog. Use the dialog notification message to explain to the user why this action was taken.

Note: The Blocking dialog is not shown for files detected by CA DataMinder Network. For these files; the user may simply see a timeout.

Available Actions: Data At Rest

Data At Rest actions apply to scanned files (that is, files scanned by the FSA). If a scanned file triggers Data At Rest policy, you can capture the file attributes (but not the file itself). Alternatively, you can silently delete the file or replace the file with an explanatory stub file. The available actions are:

Report

CA DataMinder captures the file attributes, though not the file content, and stores them on the CMS. No other action is taken.

Replace with Stub File

If CA DataMinder detects an unauthorized file, it silently deletes the file and replaces it with an explanatory stub file to alleviate any user concerns. You can customize the stub file's text content for each policy.

When you use this Replace action in combination with the 'Copy File To' global option, this action effectively becomes a Move action.

Delete

If CA DataMinder detects an unauthorized file, it silently deletes the file.

When you use this Delete action in combination with the 'Copy File To' global option, this action effectively becomes a Move action.

Global Option

You can also specify a 'Copy File To' location for each of the above actions.

Who Do the Standard Policies Apply To?

The iConsole standard policies only apply to members of the FPP Custom group or its subgroups.

More information:

[FPP User Groups Created Automatically on the CMS](#) (see page 98)

FPP User Groups Created Automatically on the CMS

When you install the iConsole standard policies, two user groups are created automatically below the top-level Users group:

FPP Base Group

This user group functions as a receptacle for the default FPP policies. It does not contain any user accounts.

FPP Custom Group

The policy for this group gets updated when you edit the policies in the iConsole. This group contains new user accounts created automatically when you install CA DataMinder endpoint agents. This group also contains various accounts used by CA DataMinder to apply policy to file events and unrecognized email senders.

User Accounts in FPP Custom Group

The following user accounts are added, or moved to, the \FPP Custom Group folder:

New users

After installing the iConsole standard policies, any new CA DataMinder user accounts created when you deploy CA DataMinder endpoint agents are added to the FPP Custom Group.

Note: Any CA DataMinder user accounts that already existed before you installed the iConsole standard policies are **not** moved to the FPP Custom Group. These user accounts stay in their existing users groups and are not governed by the iConsole standard policies. The standard policies only apply to users in the FPP Custom Group and its subgroups.

UnknownInternalSender

This account has no management or administrative privileges; its sole purpose is as a conduit to enable policy engines to apply policy to internal emails from unrecognized senders.

When you install a CMS, the Unknown Internal Sender setting in the machine policy defaults to this UnknownInternalSender user account

DefaultFileUser

This account has no management or administrative privileges; its sole purpose is as a conduit to enable policy engines to apply policy to scanned, captured or imported files if no other means are available to determine the policy participant.

When you install a CMS, the Default Policy for Files setting in the machine policy defaults to this DefaultFileUser user account.

DefaultClientFileUser

This account is similar to the DefaultFileUser account. The account is used solely by the Client File System Agent (CFSA) when scanning local workstations. The CFSA uses this account to apply the same policy to scanned files across all workstations.

When you install a CMS, the Default Policy for Data At Rest setting in the machine policy defaults to this DefaultClientFileUser user account.

Editing Policy in the iConsole

You can edit the standard policies in the iConsole.

To edit policies in the iConsole

1. Log onto the iConsole using a CA DataMinder account with appropriate administrative privileges. In particular, your CA DataMinder account must have the 'Policies: Edit Policy' privilege.

Note: FastStart users must log on using the Primary Administrator account. The credentials for this account were supplied when the Base Package was installed.

2. Go to the Policy tab and select the policy document that you want to edit.

A *policy document* is a collection of predefined user policies, such as the CA Foundation Policy Pack (FPP) or Autonomy Message Manager policy documents. Policy documents are customizable and enable you to quickly roll out CA DataMinder policies across your organization.

Within a policy document, individual policies are typically organized into *policy classes*. Each class contains the individual policies that target specific types of information or data. For example, the 'Personally Identifiable Information (PII)' class contains the FPP 'Account Number' and 'Credit Card Information' policies.

3. In the Edit Policy Document page, you can:
 - Edit the Global Options. Double-click the option that you want to edit.
 - Enable or disable triggers for individual policies. Select or clear the relevant checkboxes.
 - Edit the settings for individual policies or triggers. Double-click the policy that you want to edit.
4. Click the Save button in the Edit Policy Document page to save all the changes to the policy document.

Important! You must edit these policies in the iConsole! If you edit them directly in the Administration console, there may be unexpected results. Specifically, do not use the Policy Editor in the Administration console to edit policy for the top-level 'Users' group, FPP Base group, FPP Custom group, or any user in the FPP Custom group.

More information:

[Define the Global Options](#) (see page 101)

[Enable Policy Triggers](#) (see page 102)

[Edit the Policy Settings](#) (see page 103)

[Choose a Policy Action](#) (see page 104)

[Save the Policy Changes](#) (see page 104)

Define the Global Options

Global options are settings that apply to all applicable policies. For example, you can specify a target folder for any scanned files that need to be copied to safe location.

To edit the global options

1. Go to the Policy tab.
2. Double-click the policy pack that you want to edit.

For example, the Standard Policy Pack global options are:

Action Configuration: Data At Rest

Apply to files scanned by the FSA or CFSA. If required, you can copy scanned files to any specified folder. You can specify separate target folders for emails for Report, Replace and Delete actions.

Action Configuration: Data In Motion - Email

Apply to emails detected by any CA DataMinder email agent or any inbound or outbound e-mails detected by CA DataMinder Network. If required, you can forward these emails to another address. For example, you can forward inappropriate emails to a manager. You can specify separate forwarding addresses for different policy actions (Monitor, Encrypt, Warn or Block).

Security Officer Contact Information

Specify the name and contact telephone number for a security officer. This contact information is automatically included in any messages shown to users as a result of policy processing (for example, when an email generates a warning), enabling the user to directly contact the security officer if necessary.

Miscellaneous: Internal Domains Variable

Specify a list of internal domains. When CA DataMinder analyzes an email, if a recipient's email address matches the specified internal domain, the email is flagged as internal.

Miscellaneous: Global Policy Variables

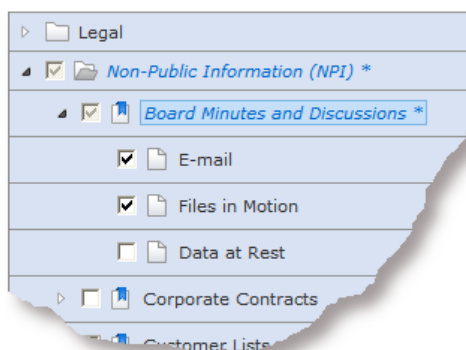
Define various lists and values that apply to all policies. For example, you can define a list of excluded file types which are always exempted from policy processing.

Enable Policy Triggers

By default, all policies are disabled. More accurately, the triggers for each policy are disabled. You now need to enable those policies and triggers that you want to use.

To enable policy triggers

1. In the Edit Policy Documents page, find the policy you want to edit.
2. For each policy, separate triggers are available for e-mails, network traffic and files. To enable or disable a policy, select the relevant checkboxes:



Email

Apply to outgoing e-mails detected by a CA DataMinder email agent or any inbound or outbound emails detected by CA DataMinder Network.

Files in Motion

Apply to network traffic passing through the CA DataMinder Network Appliance and files being printed or copied to a removable device (detected by the Client File Print Agent or Client File Save Agent respectively).

Data at Rest

Apply to scanned files, items on SharePoint sites, and items in Exchange public folders.

Edit the Policy Settings

You can edit the individual settings for each policy you want to use. For example, in the Account Number policy you can specify words that, if detected, exempt the email or document and prevent the policy from firing.

To edit policy settings

1. In the Edit Policy Documents page, find the policy you want to edit.
2. Double-click the policy to open the Policy page.

This contains the editable settings for the current policy, organized into separate tabs.

Common Content tab

Contains settings applicable to all triggers in this policy.

Many policies include a **Sensitivity** setting:

- Policies with **Lowest** sensitivity only fire if there is strong evidence that an email or file breaches policy. Set a low sensitivity if you want to reduce false positive alerts,
- Policies with **Highest** sensitivity require less evidence that policy has been breached and so fire more readily. Set a high sensitivity if you want to ensure that no incidents are missed.

Note: In technical terms, Sensitivity settings are based on the MinScore(n) classifier function.

Data In Motion - Email tab

Contains trigger settings and the policy action for emails detected by a CA DataMinder email agent or by CA DataMinder Network.

Data In Motion - Network/Endpoint tab

Contains Data In Motion trigger settings and policy action for files being printed, copied to a removable device, or detect while passing through the CA DataMinder Network appliance.

Data At Rest tab

Contains Data At Rest trigger settings and policy action for files scanned by the FSA or CFSA.

3. Edit the settings as required, then close the Policy page.

Choose a Policy Action

For each trigger, there is a drop-down list of available actions.

To choose a policy action

1. In the Edit Policy Documents page, find the policy you want to edit.
2. Double-click the policy to open the Policy page.
3. Go to the relevant trigger tab (for example, Data In Motion - Email).
4. Edit the 'Apply the following action' field.

Emails

You can block emails, warn the user, enforce or advise email encryption, or monitor emails.

Files In Motion

You can block files, warn the user, enforce or advise file encryption, or monitor file activity.

Data At Rest

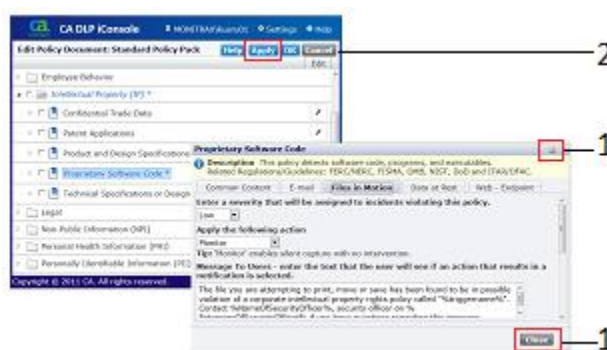
You can 'report' unauthorized files (that is, capture the file details but take no other action). Or you can remove files and replace them with explanatory 'stub' files. Or you can simply delete files.

Save the Policy Changes

After editing your triggers, you must save your policy changes.

To save policy changes

1. After editing the policy settings, click a Close button (1) to quit the Policy page and return to the Edit Policy Document Page.



2. In the Edit Policy Document page, click the Apply button (2).

Important! Do not log off without saving your changes.

Policy Tuning

The customizations in the following sections let you control the efficiency of an individual policy.

More information:

[Basic Rules](#) (see page 105)

[Matching Numbers](#) (see page 106)

[Ignore Key Words When They Occur in Disclaimers](#) (see page 107)

[Words That Indicate a Definite Non-Match](#) (see page 108)

[Positive Indicators](#) (see page 109)

[Threshold Values](#) (see page 109)

Basic Rules

When editing policies in the iConsole, be aware of the basic rules for matching search terms and the supported syntax for constructing search expressions.

Whole words

The policy matches only whole 'words'. So **unipr** does not match **Unipraxis**, and **1500** will not match **15006**.

Case

Matching is not case-sensitive. So **unipraxis** matches **Unipraxis**.

Spaces

Spaces are handled as literal characters, so spaces between words create a single, composite search term.

For example, if the search text is **unipraxis solutions**, the policy confirms a match if it detects the phrase 'Unipraxis solutions'. Any differences in capitalization are ignored.

Hyphens

By default, a policy ignores the hyphen in hyphenated words. So **##work-force%** matches any of the following:

work-force, workforce, work force

Other occurrences of hyphens are not ignored but handled as literal characters. For example, **##A-1-\d%** matches **A-1-3** but not **A 1-3** or **A 1 3**.

Matching Numbers

You can match specific numbers exactly, for example, 100, 1506, 867-5309 ('literal matching') or you can match against a *template* (for example, 'match any 5-digit number joined by a hyphen to a 4-digit number').

Syntax

Templates only: %# ... %

This syntax is mandatory when specifying a *character template* or *number template*. It matches the contained template on a per character basis.

Separate multiple templates with commas:

%#<template>%, %#<template>%

This syntax is not needed for literal matching.

\a or \A

Matches any single letter

\d or \D

Matches any single digit (0-9)

\l or \L

Matches any single letter or digit

\p or \P

Matches any single punctuation character

[M]

Matches M occurrences of a character. For example, **\d[3]** matches any 3 digit number.

[M,N]

Matches M to N occurrences of a character. For example, **\d[1,5]** matches any number with between 1 and 5 digits

[[a-z]]

Matches any character between 'a' and 'z'. Use this syntax to limit the range of permitted character matches.

Examples

867-5309

This number matches 867-5309 only; it does not match, for example, 5309, or 467-5309.

%#\d[5]\a[3]-\d[5,7]%

This template matches any string of 5 digits followed by 3 letters, followed by a hyphen and 5 to 7 digits. For example, 32456dfs-345661.

%#\d[3]{.-| }\d[4]%

This template matches 7 digit telephone numbers where the first three digits are separated by a period, a dash, or a space. For example, 021-7657 or 021 7657.

%#[[2-5]]\d[11,13]%

This template matches any numeric string that starts with 2, 3, 4, or 5, and is followed by 11 to 13 digits. For example, 398744614630.

%#22\a[2]\d[1,4]\p [[x-z]]%

This template matches the number 22, followed by exactly two letters, then 1 to 4 digits, joined to punctuation, then followed by a space and the letter x, y, or z. For example, 22AB123. Z.

Ignore Key Words When They Occur in Disclaimers

In the Non-Public Information policy group, the Information Security Label Control policy includes a 'disclaimer exemption' field. This field enables you to exempt words or phrases that are permitted if detected in a corporate disclaimer but which, in any other context, would cause a policy to fire.

As a minimum, you need to specify, with complete accuracy, the entire sentence containing the key words, plus any punctuation, exactly as they are found in the disclaimer. For greater accuracy, include the sentence (plus punctuation) that immediately follows the triggering sentence. For maximum accuracy, include the entire disclaimer plus punctuation. Repeat this process for each triggering word or phrase that appears in the disclaimer, even if these occur in the same sentence. For example, if the disclaimer includes two triggering phrases, for maximum accuracy you would need to enter the full disclaimer twice in the 'disclaimer exemption' field.

Example 1

"This email is the **private property** of the sender and is meant **for the intended recipient** only. If you are not that individual, and have received this email in error, please notify the sender and destroy the communication. Please do not discuss its contents with anyone."

In this example, policy is configured to fire on the bold phrases. To exempt these phrases when they appear in a disclaimer, you would need to enter the first sentence two times in the 'disclaimer exemption' field. This is because triggering phrases occur twice in one sentence.

Example 2

"This email is the **private property** of the sender. It is meant **for the intended recipient** only. If you are not that individual, and have received this email in error, please notify the sender and destroy the communication. Please do not discuss its contents with anyone."

In this example, the triggering phrases occur in separate sentences. This time, you can enter both sentences once each or, for maximum accuracy, include the entire disclaimer twice.

Words That Indicate a Definite Non-Match

Many policies include an Immediate Disqualifier field. If CA DataMinder detects any Immediate Disqualifier words or phrases in an email, file, or web page, this immediately results in a non-match. That is, the item definitely does not match the policy criteria. CA DataMinder does not apply policy to these items even if they contain other sensitive words or phrases.

If an Immediate Disqualifier word or phrase is detected in an:

- **Email attachment**, the attachment is excluded from policy but policy may still be applied to the email subject and body text. Likewise, if a key word or phrase is detected in the subject or body text, policy may still be applied to any attachments.
- **File**, the entire file is excluded from policy.

You typically use Immediate Disqualifier words or phrases to:

- Exclude communications that are exempt from policy, such as documents containing specific disclaimers, copyright notices, or unique identifiers.
- Create a 'pass code' that allows safe communications (such as pre-approved forms or marketing reports) to be sent without triggering policy. The pass code must be a phrase or other code that would not normally appear in a business document or email. Pass codes can be used to allow individuals, such as compliance monitors, to bypass policy.

Important! Extreme care is needed when choosing pass codes and other definite non-match words. Any user who is aware of a pass code could intentionally include it in an inappropriate communication to deliberately avoid detection. Likewise, using a non-unique term as the pass code will undermine the effectiveness of the policy.

Positive Indicators

Many policies include a Positive Indicator field. This field defines a list of preferred words or phrases. If CA DataMinder detects a Positive Indicator word or phrase in an email, file, or web page, this increases the probability that the item matches the policy criteria.

Threshold Values

Some Threshold policies analyze emails and files to calculate a document score. This score quantifies how closely an email matches the policy criteria; if the document score equals or exceeds a minimum value (the 'default threshold value'), the policy fires.

For these policies, you can override the default threshold value by editing the Threshold Value policy field. In particular, if this default value is causing too many false positives, you can raise the default value to make the policy more stringent. But if you do raise the default value, you must increase it by at least 2 or 3 to offset any 'definite indicator' words or phrases built into the policy which, if detected in a file or email, will automatically increment the document score.

The policies that you can edit and their minimum threshold increases are listed below:

PII (Personally Identifiable Information)

Account Number - Threshold

The default Threshold Value is 7. Increase this by +3.

Credit Card Information - Threshold

The default Threshold Value is 7. Increase this by +2.

Social Security Number - Threshold

The default Threshold Value is 7. Increase this by +3.

US Individual Taxpayer Identification Number (ITIN) - Threshold

The default Threshold Value is 6. Increase this by +2.

PHI (Personal Health Information)

Medical Record Numbers - Threshold

The default Threshold Value is 7. Increase this by +2.

NPI (Non-Public Information)

Customer Lists

The default Threshold Value is 20. Increase this by +2.

Chapter 7: Exempting Users From Policy

You can exempt users from policy so that CA DataMinder does not monitor the activity of these users.

This section contains the following topics:

[Exempt Users](#) (see page 111)

[Manually Exempt Users From Policy](#) (see page 112)

Exempt Users

(Only applicable for users with licenses such as CA DataMinder Express)

Exempt users are users who have a CA DataMinder account on the CMS but who are exempt from policy. That is, CA DataMinder does not monitor email, web or file activity for policy-exempt users.

Most importantly, exempt users are not included in your licensed user count. For example, if your CA DataMinder license allows 100,000 users, your CMS is permitted to store user accounts for 100,000 licensed users *plus* an unlimited number of exempt users.

Why Do I Need Exempt Users?

If you deploy CA DataMinder endpoint agents on a shared computer (for example, in a hot desking environment), a new CA DataMinder user account is created automatically each time a new user logs onto that computer. In an organization with many shared computers, this can result in more user accounts than your CA DataMinder license permits. In turn, this can mean that some users are not subject to policy control even if you want them to be.

Even if you delete an unwanted CA DataMinder account in the Administration console, CA DataMinder automatically recreates the account if that user logs into Windows again on any CA DataMinder computer.

If you have users in your organization who are not subject to CA DataMinder policy control, you can exempt these users from policy to avoid exceeding your maximum number of licensed users.

How Do I Create Exempt Users?

You can manually exempt users from policy. In effect, you convert a licensed user account to an exempt user account.

You can also automatically exempt specific users from policy when you run an Account Import job. For example, you can exempt any user accounts imported from your LDAP directory and which have a specific LDAP attribute.

Manually Exempt Users From Policy

You can manually exempt users from policy. You can also manually undo a policy exemption.

To exempt users from policy

1. Log on to the Administration console using an account that has the 'Users: Edit the user hierarchy' administrative privilege.
2. Expand the User Administration branch and select the users who you want to exempt from policy.
3. Click Tools, Set Policy Exemption.

The Select Policy Exemption State dialog appears.

4. Select the Exempt From Policy check box and click OK.

To undo a policy exemption

1. Log on to the Administration console using an account that has the 'Users: Edit the user hierarchy' administrative privilege.
2. Expand the User Administration branch and select the policy-exempt users who you want to apply policy to.
3. Click Tools, Set Policy Exemption

The Select Policy Exemption State dialog appears.

4. Clear the Exempt From Policy check box and click OK

Chapter 8: Intervention Setting

In the user policy, each control action, whether for emails, files, Web pages or application monitoring, contains a version of the Intervention setting.

This setting is the pivotal determinant in the control procedure and determines the type of control event. The Intervention option that you choose determines whether to block, warn or inform the user, encrypt, delete or replace a file, quarantine emails, categorize events, remove or replace scanned files, or silently monitor user activity.

This section contains the following topics:

- [Supported Intervention Options by Client](#) (see page 113)
- [Supported Intervention Options: Email Server Agents](#) (see page 114)
- [Intervention Setting: Advise Encryption](#) (see page 116)
- [Intervention Setting: Block with Notification](#) (see page 117)
- [Intervention Option: Block Quietly](#) (see page 118)
- [Intervention Option: Block \(File Events\)](#) (see page 119)
- [Intervention Option: Categorize - Single Category Only](#) (see page 119)
- [Intervention Option: Categorize - Multiple Categories Allowed](#) (see page 120)
- [Intervention Option: Categorize](#) (see page 120)
- [Intervention Option: Delete \(Scanned Files\)](#) (see page 121)
- [Intervention Option: DoD Overwrite and Delete](#) (see page 121)
- [Intervention Option: DoD Overwrite and Replace](#) (see page 122)
- [Intervention Setting: Enforce Encryption](#) (see page 123)
- [Intervention Option: Inform](#) (see page 124)
- [Intervention Option: No Further Actions](#) (see page 125)
- [Intervention Option: None](#) (see page 125)
- [Intervention Option: Notify](#) (see page 126)
- [Intervention Option: Quarantine Quietly](#) (see page 127)
- [Intervention Option: Quarantine with Notification](#) (see page 128)
- [Intervention Option: Replace](#) (see page 129)
- [Intervention Option: Warn](#) (see page 129)
- [Intervention Option: Warn \(Personal\)](#) (see page 130)

Supported Intervention Options by Client

The following Intervention options are supported for the CA DataMinder Microsoft Outlook endpoint agent and CA DataMinder Lotus Notes endpoint agent.

Intervention	Outlook agent	Notes agent
Silent Capture	Yes	Yes
Warn	Yes	Yes

Intervention	Outlook agent	Notes agent
Quarantine with notification	Yes	Yes
Quarantine quietly	No	No
Block with notification	Yes	Yes
Block quietly	Yes	Yes
Move recipients to BCC	Yes	No
X-header tagging	Yes	Yes
Detect direction	Yes (incoming/outgoing)	Yes (incoming/outgoing)
Encrypt	Yes	Yes

Supported Intervention Options: Email Server Agents

The CA DataMinder email server agents include the Exchange server agent, Domino server agent, IIS SMTP agent, and Milter MTA agent (for Sendmail and Postfix). These agents support the following Intervention options.

Intervention	Microsoft Exchange	Lotus Domino	IIS SMTP	Milter MTA	NBA
Silent capture	Yes	Yes	Yes	Yes	Yes
Warn	Yes	No	Yes	No	No
Quarantine with notification	Yes	Yes	Yes	Yes (2)	Yes (2)
Quarantine quietly	Yes	Yes	Yes	Yes (2)	Yes (2)
Block with notification	Yes	Yes	Yes	Yes	Yes
Move recipients to BCC	No	No	No	Move "all" only	No
X-header tagging	Yes	Yes	Yes	Yes	No
Reprocess emails (1)	Yes (Outlook agent)	Yes (Notes agent)	Yes (Outlook agent)	No	No
Detect direction	Server agents always apply outgoing email triggers.				
Encrypt	Yes (3)	Yes (3)	Yes (3)	Yes (3)	No

- (1) Checks WiganStatus property to see if the email has already been processed by the specified CA DataMinder endpoint agent. You can optionally configure a server agent to reprocess an email if it has already been processed.
- (2) Does not quarantine internet mails containing TNEF data.
- (3) Server agents only support Enforce Encryption (not Advise Encryption).

Intervention Setting: Advise Encryption

Available for: Outgoing Emails; Data In Motion events detected by CFSA.

Not available for: Incoming Emails; Data At Rest events; events detected by the NBA; events detected by the Client Network Agent (CNA). See the warning below.

Choose Advise Encryption to warn users whenever CA DataMinder detects an attempt to send an unencrypted email or copy an unencrypted file to a removable device such as a USB drive. You can specify a customized notification message for each control trigger.

Important! Do not choose this intervention option for triggers associated with the NBA or CNA.

- The NBA cannot send encryption warnings when it detects unencrypted files, webmails and SMTP emails. Consequently, such items are sent or copied without encryption.
- The CNA cannot send encryption warnings when it detects unencrypted data submissions to web sites. Consequently, items such as file uploads are submitted without encryption.

Emails

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog to the email sender. The sender can choose one of the following:

Encrypt

CA DataMinder inserts an 'encryption request' x-header into the email. This x-header is subsequently detected by a third-party encryption provider, which in turn encrypts the email before it leaves your network.

Don't Encrypt

The email is sent unencrypted.

Cancel

The email is not sent. For emails detected by a CA DataMinder email server agent:

- If server-side interactive warnings are **not** enabled, CA DataMinder does not intervene and the email is sent **unencrypted**.
- If server-side interactive warnings **are** enabled, CA DataMinder sends a warning email to the sender. If the sender replies to the warning promptly, their original email is released and sent **unencrypted** to its intended recipients. If they do not reply (or reply too late), their original email is disposed of without being sent.

Important! If server-side interactive warnings are enabled, make sure that the message to users in the warning email clearly explains the consequences of replying and not replying! In particular, note the different reply handling for the Advise Encryption and Enforce Encryption options.

Data In Motion

When the warning displays, the user copying the file can choose one of the following:

Encrypt

CA DataMinder prompts the user for a password, and uses this password to encrypt the file on the removable device.

Don't Encrypt

The file is copied onto the removable device unencrypted.

Cancel

The file is not copied.

Note: CA DataMinder cannot encrypt files being copied to network locations. Do not use Advise Encryption or Enforce Encryption control actions to prevent unencrypted files being copied to shared locations on your network.

Intervention Setting: Block with Notification

Available for: Incoming emails; outgoing emails; Application Monitor

Not available for: Data At Rest; Data In Motion. However, a Block (File Events) intervention option is available for files detected by Data In Motion triggers.

Choose Block with Notification to display the Blocking dialog whenever an email, Web page, or data submission to a Web site is blocked. You can specify customized notification messages for each control trigger.

Emails

For intended recipients, you could combine this option with a Forward Incoming Email setting to effectively redirect the email. You can use the notification message in the blocking dialog to explain what action has been taken.

For incoming emails, you can send an automatic reply to the sender and delete the email from the user's Inbox or leave it in the Inbox but with its body text replaced by a standard notification message.

Applications

For blocked applications, the application fails to start up. The mouse pointer temporarily changes to 'busy' then reverts to 'normal'.

Intervention Option: Block Quietly

Available for: Incoming emails; Application Monitor

Not available for: Outgoing emails; Data At Rest; Data In Motion. However, a Block (File Events) intervention option is available for files detected by Data In Motion triggers.

Choose Block Quietly to discreetly block incoming emails or attempts to start an application. From a user's viewpoint, the effects are as follows:

Emails

For intended recipients, their awareness of the blocking depends on the Delete or Replace setting. If this deletes blocked emails from their Inbox, the user is normally unaware that their email has been blocked (in rare cases, the blocked email may briefly appear then disappear in the Inbox). Conversely, you can configure the setting to allow blocked emails to arrive in the recipient's Inbox, but with their body text replaced by a standard notification message.

You can also forward emails to another address and send automatic replies to incoming emails.

Applications

For blocked applications, the application fails to start up. The mouse pointer temporarily changes to 'busy' then reverts to 'normal'.

More information:

[Intervention Setting](#) (see page 113)

Intervention Option: Block (File Events)

Available for: Data In Motion.

Not available for: Emails; Application Monitor; Data At Rest. However, Block Quietly and Block with Notification intervention options *are* available for emails.

Choose Block to block a file or document detected by a Data In Motion control trigger. The blocking is silent, or the user is shown a notification dialog, depending on which agent detected the file:

CFSA, CPSA, CNA

For files detected by the Client File System Agent, Client Print System Agent, or Client Network Agent, CA DataMinder displays the Blocking dialog. For example, the Blocking dialog is shown if a user tries to print an unauthorized file or copy it to a USB device. You can use the dialog's notification message to explain to the user why this action was taken.

NBA

For files detected by the Network Boundary Agent, such as uploads to a web site, CA DataMinder displays the Blocking dialog if possible. However, for some web sites, it is not possible to display a Blocking dialog and the blocking is silent.

Intervention Option: Categorize - Single Category Only

Available for: Incoming emails; outgoing emails; Data In Motion.

Not available for: Application Monitor; Data At Rest. However, a separate 'Categorize' intervention option *is* available for items scanned by Data At Rest triggers.

Choose 'Categorize - Single Category Only' to ensure that a file or email is successfully categorized. If the Categorize dialog is shown, the user can only choose a single category for their file or email.

Categorization can be automatic or manual, depending on how the control triggers are configured and, for emails, whether the email was detected by an endpoint agent or server agent.

Note: For files detected by the NBA or Client Network Agent, categorization is always automatic.

Intervention Option: Categorize - Multiple Categories Allowed

Available for: Incoming emails; outgoing emails; Data In Motion.

Not available for: Application Monitor; Data At Rest. However, a separate 'Categorize' intervention option *is* available for items scanned by Data At Rest triggers.

Choose 'Categorize - Multiple Categories Allowed' to ensure that an email or file is successfully categorized. If the Categorize dialog is shown, the user is permitted to choose multiple categories from the list.

Categorization can be automatic or manual, depending on how the control triggers are configured and, for emails, whether the email was detected by a client agent or server agent.

Note: For files detected by the NBA or Client Network Agent, categorization is always automatic.

Intervention Option: Categorize

Available for: Data At Rest.

Not available for: Incoming emails; outgoing emails; Data In Motion; Application Monitor. However, 'Categorize - Single Category Only' and 'Categorize - Multiple Categories Allowed' intervention options *are* available for these control actions.

Choose Categorize to ensure that scanned files are automatically categorized. Specifically, use this option to categorize files in a local or remote file system, in Exchange Public Folders, and files retrieved from the Microsoft SharePoint site.

With this option, file events are always categorized automatically; the Categorize dialog is never shown. If a file causes multiple triggers to fire, CA DataMinder automatically chooses the category with the highest score.

Intervention Option: Delete (Scanned Files)

Available for: Data At Rest. Note that a DoD Overwrite and Delete option is also available.

Not available for: Emails; Application Monitor; Data In Motion.

Choose Delete to delete files. These can be files located in a local or remote file system, or on Microsoft SharePoint sites. From a user's viewpoint, they will only be aware that their file no longer exists when they next try to view it. You can still capture the associated file event and copy the file to an alternative location.

You can combine this control action with a Copy action to effectively move files to a new location.

Intervention Option: DoD Overwrite and Delete

Available for: Data At Rest. But note that for items detected in Exchange Public Folders or SharePoint sites, DoD Overwrite and Delete actions are *not* supported, although Delete actions (without DoD deletions) *are* supported.

Not available for: Emails; Application Monitor; Data In Motion.

Choose DoD Overwrite and Delete to delete files, using DoD deletions to ensure deleted files cannot be recovered. These can be files located in a local or remote file system. From a user's view, they only are aware that their file no longer exists when they next try to view it. You can still capture the associated file event and copy the file to an alternative location.

You can combine this control action with a Copy action to effectively move files to a new location.

Intervention Option: DoD Overwrite and Replace

Available for: Data At Rest. But note that for items detected in Exchange Public Folders or SharePoint sites, DoD Overwrite and Replace actions are *not* supported, although Replace actions (without DoD deletions) *are* supported.

Not available for: Emails; Application Monitor; Data In Motion.

Choose DoD Overwrite and Replace to delete files using DoD deletion (see below) and replace them with an explanatory stub file to alleviate any user concerns. For example, you can inform a user that their file was inappropriate and has been removed to a new location. These can be files located in a local or remote file system.

You can combine this control action with a Copy action to effectively move files to a new location.

Intervention Setting: Enforce Encryption

Available for: Outgoing Emails, Data In Motion events detected by CFSA.

Not available for: Incoming Emails; Data At Rest events; events detected by the NBA; events detected by the Client Network Agent (CNA). See the warning below.

Choose Enforce Encryption to ensure that sensitive emails are encrypted before they are sent or that sensitive files are encrypted before they are copied to a removable device or a sync folder. When CA DataMinder detects these operations, it warns the user. The user can encrypt their email or file, or they can cancel the operation. They cannot send an unencrypted email or copy an unencrypted file.

Important! Do not choose this intervention option for triggers associated with the NBA or CNA.

- The NBA cannot enforce encryption when it detects unencrypted files, webmails and SMTP emails. Consequently, such items are sent or copied without encryption.
- The CNA cannot enforce encryption warnings when it detects unencrypted data submissions to web sites. Consequently, items such as file uploads are submitted without encryption.

Emails

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog to the email sender. The sender can choose one of the following:

Encrypt

CA DataMinder inserts an 'encryption request' x-header into the email. This x-header is subsequently detected by a third-party encryption provider, which in turn encrypts the email before it leaves your network.

Cancel

The email is not sent.

For emails detected by a CA DataMinder email server agent:

- If server-side interactive warnings are **not** enabled, CA DataMinder automatically encrypts the email before sending it.
- If server-side interactive warnings **are** enabled, CA DataMinder sends a warning email to the sender. If the sender replies to the warning promptly, their original email is released and sent **encrypted** to its intended recipients. If they do not reply (or reply too late), their original email is disposed of without being sent.

Important! If server-side interactive warnings are enabled, make sure that the message to users in the warning email clearly explains the consequences of replying and not replying! In particular, note the different reply handling for the Advise Encryption and Enforce Encryption options.

Data In Motion

When the warning displays, the user copying the file can choose one of the following:

Encrypt

CA DataMinder prompts the user for a password, and uses this password to encrypt the file on the removable device.

Cancel

The file is not copied.

Note: CA DataMinder cannot encrypt files being copied to network locations. Do not use Advise Encryption or Enforce Encryption control actions to prevent unencrypted files being copied to shared locations on your network.

Intervention Option: Inform

Available for: Incoming emails; outgoing emails; Application Monitor; Data In Motion events detected by CFSA.

Not available for: Data At Rest; events detected by the NBA; events detected by the Client Network Agent (CNA).

Choose Inform to display an advisory dialog whenever CA DataMinder detects email, file, or application activity that is potentially significant. This option is useful if, for example, you want to remind users that their activity is being monitored, or you want to notify users when specified emails arrive in their inbox,. You can specify customized notification messages for each control trigger.

Incoming Emails and Application Monitor

When incoming emails arrive or when specified applications start up, the Inform dialog has a single OK button. If a user clicks OK, this generates a 'disregarded inform' control event.

Outgoing Emails

The Inform dialog has Continue and Cancel buttons. If the sender clicks:

- Continue, the user is allowed to send the email. This generates a 'disregarded inform' control event.
- Cancel, the user can amend the email before sending. This generates a 'heeded inform' event.

Data In Motion file events

The Inform dialog displays when a user tries to print a file or copy files to a removable drive. The dialog has a single OK button. If the user clicks OK, the user is allowed to print or copy the file.

Intervention Option: No Further Actions

Available for: Incoming emails; outgoing emails; Application Monitor; Data In Motion; Data At Rest.

Not available for: Always available.

Choose No further actions to stop any further control actions being applied whenever CA DataMinder detects specific email, file, or application activity. CA DataMinder immediately stops processing the event and no further policy actions are performed (for example, forwarding an email or sending a reply).

If you set No Further Actions as the first control action, you can use it to filter out spam emails without using Include and Exclude lists. CA DataMinder can also exempt specific files or applications.

Intervention Option: None

Available for: Incoming emails; outgoing emails; Application Monitor; Data In Motion; Data At Rest.

Not available for: Always available.

Choose None to generate a silent event whenever CA DataMinder detects unauthorized email, file, or application activity. This means that CA DataMinder silently records these events without blocking them or displaying a warning, or without deleting or replacing the original file. The user is completely unaware that their activity has triggered a control event.

For example, a humorous but inoffensive email attachment is circulating within your organization and your bandwidth is suffering. Configuring your control actions to generate silent events lets you discreetly trace the source of these emails without resorting to blocking users and the attendant risk of offending your workforce.

In all cases, you can capture the associated event. You can also forward emails to another address and send automatic replies to incoming emails.

Intervention Option: Notify

Available for: Incoming emails.

Not available for: Outgoing emails; Application Monitor; Data At Rest; Data In Motion.

Choose Notify to display an advisory dialog whenever an email of interest arrives in a user's Inbox. This is the same as the advisory dialog used by Inform events, but Notify events have some important differences. In particular, Notify events occur when an email is received; Inform events occur when a user opens or previews the email. The handling of Notify events also varies according to the email system running on the machine receiving the email:

Microsoft Outlook

If Outlook is configured so that emails stay in your mailbox on the Exchange server, then any emails that arrive while Outlook is not running (for example, overnight) will not trigger a Notify event.

But if Outlook is configured to migrate emails down into your Personal Folders, Outlook must be running for the advisory dialog to appear. This means that if any advisory-triggering emails arrive while Outlook is not running (for example, overnight or while you are on holiday), you may be greeted by a flurry of notifications when you next start up Microsoft Outlook!

Lotus Notes

If you connect to your mail directly on a Domino Notes server, an incoming email cannot trigger a Notify event.

But if you have a local mail file, with regular replication between the Domino Notes server and your local database, then a Notify event is triggered when the incoming email is replicated to your local database.

Note: Notify actions cannot be invoked if the trigger requires access to the email content but the email is digitally signed or encrypted.

Intervention Option: Quarantine Quietly

Available for: Outgoing emails.

Not available for: Incoming emails; Application Monitor; Data At Rest; Data In Motion.

Choose Quarantine quietly to silently quarantine emails that require urgent review without notifying the senders. That is, the sender remains unaware that their email has not been sent to its intended recipients.

After the email has been reviewed, it is released from quarantine and sent on to its recipients, or it is rejected and not sent. In both cases, the email is retained in the CMS database.

Intervention Option: Quarantine with Notification

Available for: Outgoing emails.

Not available for: Incoming emails; Application Monitor; Data At Rest; Data In Motion.

Choose Quarantine with notification to quarantine emails that require urgent review and to notify the sender that this has happened and that the email has not been sent to its intended recipients. This option is useful if you want to educate your users on acceptable email usage. The text in the advisory message is fully customizable.

After the email has been reviewed, it is released from quarantine and sent on to its recipients, or it is rejected and not sent. In both cases, the email is retained in the CMS database.

Advisory message guidelines

Different guidelines apply, depending on whether an email is quarantined by an endpoint agent or server agent:

Email server agents

When an email is sent and subsequently quarantined, it initially appears to the sender as though their email has been sent as normal. However, they soon receive a notification email.

The message in the quarantine notification email only needs to inform the sender that their message has been quarantined pending approval by a reviewer.

Email endpoint agents

When a user sends an email that is subsequently quarantined, the 'compose message' window stays visible on their screen. Therefore, you must edit the message in the notification dialog so it:

- Informs the user that their email has been sent, but that it has been quarantined pending approval by a reviewer.
- Instructs the user to close the compose message window and to not resend the email.

Intervention Option: Replace

Available for: Data At Rest. Note that DoD Overwrite and Replace actions are also supported.

Not available for: Emails; Application Monitor; Data In Motion.

Choose Replace to delete files and replace them with an explanatory stub file to alleviate any user concerns. For example, you can inform a user that their file was inappropriate and has been removed to a new location. These can be files located in a local or remote file system, or on Microsoft SharePoint sites.

You can combine this control action with a Copy action to effectively move files to a new location.

Important! Be aware that for items detected in Exchange Public Folders, a 'Replace' action will delete each item, but will not replace it with an explanatory stub file. A warning is written to the Activity log.

Intervention Option: Warn

Available for: Incoming emails; outgoing emails; Application Monitor; Data In Motion events detected by CFSA or CPSA.

Not available for: Data At Rest; events detected by the NBA; events detected by the Client Network Agent (CNA).

Important! Do not choose this intervention option for triggers associated with the NBA or CNA. These agents cannot display warnings.

Choose Warn to display the Warning dialog whenever CA DataMinder detects unauthorized activity. You can specify customized warning messages for each control trigger. The warning dialog lets the user choose whether to continue or not.

Cancel

If the user clicks Cancel, this generates a heeded warning. In effect, the user accepts the warning and quits what they were trying to do, for example, printing a file, sending an email, or starting up a prohibited application.

Continue

If the user clicks Continue, this generates a disregarded warning. The user is allowed to continue (for example, they can open or send the email anyway, or copy a file to a USB device), but CA DataMinder records the fact that the user did this despite being explicitly warned against doing so.

Note: A disregarded warning does not necessarily imply any misconduct by the user. For example, a user may want to send a non-encrypted email, in breach of corporate guidelines, because it concerns a trivial matter.

In all cases, you can capture the associated event, forward emails to another address and send automatic replies to incoming emails.

Intervention Option: Warn (Personal)

Available for: Emails detected by endpoint agents.

Not available for: Application Monitor; Data At Rest; Data In Motion. Also, this warning option is *not* available for emails detected by email server agents, or for SMTP emails and webmails detected by the NBA.

Choose 'Warn, user may designate as personal' to display a modified Warning dialog whenever CA DataMinder detects an email. Like the standard Warning dialog, the modified dialog lets the user choose whether to continue or not. Most importantly, the user can flag the event as 'Personal'. There are three dialog buttons:

Personal

Users can click this button to indicate that they are opening or sending a personal email. This overrides the warning, and allows the user to continue. It also generates a 'disregarded warning' event, although the event itself is identified as a personal email in the Console.

Important! If the user clicks Personal, the email content is not captured, even if the control action setting Capture Disregarded Warnings? is set to True.

Cancel

If the user clicks Cancel, this generates a heeded warning. In effect, the user accepts the warning and quits trying to send or open the email.

Continue

If the user clicks Continue, this generates a disregarded warning. The user is allowed to continue (for example, they can send the email anyway), but CA DataMinder records the fact that the user continued despite being explicitly warned against doing so.

Note: A disregarded warning does not necessarily imply any misconduct by the user. For example, a user may want to send a non-encrypted email, in breach of corporate guidelines, because it concerns a trivial matter.

In all cases, you can capture the associated event. You can also forward emails to another address and send automatic replies to incoming emails.

More information:

[Intervention Setting](#) (see page 113)

Chapter 9: Detecting Key Text

CA DataMinder uses the term 'search text' to mean the key words and phrases that you want a trigger to detect. Triggers can detect 'search text' in emails, files, Web events and IM conversations. Trigger settings such as 'Included Search Text' let you define the search text for a specific trigger.

For example, you can capture any email attachment containing the phrase 'Unipraxis sales forecast'. You can also use wildcards and variables to precisely define your search text.

This section contains the following topics:

[Basic Rules](#) (see page 134)

[Special Characters](#) (see page 137)

[Hyphenated Words](#) (see page 138)

[Far Eastern Characters](#) (see page 138)

[Which Files Can be Searched For Key Text?](#) (see page 139)

[Searching Zip Files for Key Text](#) (see page 140)

[Searching Embedded Emails for Key Text](#) (see page 142)

[Search Text Variables](#) (see page 142)

[Setting a File Size Limit](#) (see page 143)

Basic Rules

When a trigger detects key words or phrases, it applies the following rules:

Whole Words

A trigger only matches whole words. So *unipr* does not match *Unipraxis*.

Special Characters

Some characters require special handling. To detect them in their literal sense, you must 'escape' them with a '\' backslash character. These special characters are:

{ } | [] % ? * \

See the following sections for details.

Spaces

CA DataMinder matches spaces between words. Such spaces create a single, composite search term. So if the search text is *unipraxis solutions*, the trigger confirms a match if it detects the phrase *unipraxis solutions*.

But by default, CA DataMinder ignores other spaces when searching for key words or phrases. These other spaces include tabs, line breaks, and spaces next to numbers or punctuation.

Case-sensitive

By default, matching is not case-sensitive. So *unipraxis solutions* matches *Unipraxis Solutions*.

Hyphenated Words

By default, a trigger ignores the hyphen in hyphenated words. So *email* matches *email* and *e-mail*.

Punctuation

By default, a trigger matches punctuation when searching for key words or phrases, so *Unipraxis Win!!* matches *Unipraxis Win!!* but not *Unipraxis Win!* or *Unipraxis Win*. However, you can disable punctuation matching if you require more flexible matching. This can arise if your key words or phrases are frequently used with incorrect or inconsistent punctuation.

Wildcards

You can use wildcard characters * and ? when you define a list of trigger words or phrases. Substitute * for zero or more characters. Substitute ? for a single character. For example, *ref???* matches words such as *ref328*.

File Size

You can set a maximum size for files being searched to prevent excessive memory usage.

More information:

[Included, Excluded, and Ignored Items](#) (see page 64)

[Special Characters](#) (see page 384)

Wildcards and Policy List Items

CA DataMinder supports the * and ? wildcards in policy list items. You can substitute * for zero or more characters; you can substitute ? for a single character. The following table provides examples:

List items	Notes
URLs	* characters are added are automatically to start and end of these items.
unipraxis	Interpreted to be the same as *unipraxis*. The trigger detects sites such as unipraxis.com, unipraxis.co.uk or even sales.unipraxis.com.
sales.*.com	Detects sites such as sales.unipraxis.com.
Email addresses	Email address matching is not case-sensitive. CA DataMinder interprets a space between address components as AND operators.
*@unipraxis.com	Detects emails sent to or from this domain only.
@unipraxis	Detects emails sent to or from domains such as unipraxis.com or unipraxis.co.uk.
unipraxis.com	Detects any email addresses ending in 'unipraxis.com'. In effect, this is the same as specifying *@unipraxis.com.
frank unipr*	Detects all emails sent to or from, for example, frank.schaeffer@unipraxis.com.
Card numbers	CA DataMinder ignores spaces so, if you prefer, you can omit spaces between digit groups, for example, 45449?00*.
4544 9?00 *	If part of an Included list, the trigger activates whenever CA DataMinder detects a number such as 454491000000. If part of an Excluded list, the trigger is activated whenever CA DataMinder detects any card number except 454491000000.
Text	Trigger text can apply to the content of a file, Web page, email or email attachment, plus data submitted to a Web site using an HTML form.
unipr* or ref???	If part of an Included list, the trigger activates whenever CA DataMinder detects words such as Unipraxis or ref328.
holiday req*	If part of an Excluded list for an email content trigger, the trigger activates for all emails except those that contain phrases such as 'holiday request'.

List items	Notes
photocop*	If part of an Excluded list for a submitted data trigger, the trigger activates for all data submissions except when, for example, a user selects 'Photocopier paper' from a form menu.
File names	These include email attachments, imported files, and files uploaded to a Web site.
plan??? or *.xls	If part of an Included list, the trigger activates whenever CA DataMinder detects a file such as plan_13.xls.
*.jpg	If part of an Excluded list, all uploaded files activate the trigger unless this involves a file such as cute_kittens.jpg. Note: Most triggers that use file lists are activated when a listed file is detected; you can specify any file types in these list settings. But other triggers attempt to search the content of the listed files; for these triggers, only certain file types are supported in the file list.
Window titles	Used in Application Monitoring triggers. Note that * characters are added are automatically to start and end of these items.
Notepad	Interpreted to be the same as *notepad*. If part of an Included list, the trigger activates whenever a Notepad window opens.
.do? - Micro	Detects window titles such as 'planning.doc - Microsoft Word'. If part of an Excluded list, the trigger activates whenever a window opens unless it has a title such as 'planning.doc - Microsoft Word'.
Executable paths	Used in Application Monitoring triggers. Note that * characters are added are automatically to start and end of these items.
Notepad	Interpreted to be the same as *notepad*. If part of an Included list, the trigger activates whenever Notepad.exe runs.
?:*\Foo	This detects any instance of Foo.exe running in a subfolder. If part of an Excluded list, the trigger activates whenever any application runs except for, for example, C:\Program Files\Foo.exe. Note: This does not detect instances of Foo.exe running in the root of a drive, for example, H:\Foo.exe.
Special characters	To search for literal occurrences of the characters { } * or ?, prefix them with a '\' backslash. For example:
24*7	This detects 24*7.
What next for Unipraxis\?	This detects What next for Unipraxis?

Note: CA DataMinder interprets a space between keywords as a literal character except in email address and credit card number lists.

Special Characters

The following characters have special meaning:

{ } | [] % ? * \

To search for literal occurrences of these characters, you must prefix them with a \ backslash.

Note: Forward slashes are not special characters and do not need a backslash prefix. For example, you need only type 24/7 to detect '24/7'.

Examples

What next\?

If this example is part of an Included list, the trigger activates whenever CA DataMinder detects:

What next?

24*7

If this example is part of an Included list, the trigger activates whenever CA DataMinder detects:

24*7

The files are located in the \\Sales directory

If this example is part of an Included list, the trigger activates whenever CA DataMinder detects:

'The files are located in the \Sales directory'.

Note: To search for literal occurrences of backslash characters, you must still prefix them with a further backslash. This is why you must type \\Sales to detect '\Sales'.

The domain you need is: unipraxis\\srimmel

If part of an Included list, the trigger activates whenever CA DataMinder detects:

'The domain you need is: unipraxis\srimmel'

More information:

[Search Text Syntax](#) (see page 383)

Hyphenated Words

By default, CA DataMinder ignores the hyphen in hyphenated words when searching for key words or phrases. This provides built-in flexibility to detect variations of words that are inconsistently hyphenated. For example:

- **Example:** *e-mail* matches *e-mail* or *email*.
- **Example:** *email* matches *email* or *e-mail*.

Note: CA DataMinder does not ignore other occurrences of hyphens. For example, the search text *Recruitment - May 2010* only detects an exact match of this phrase, that is, "*Recruitment - May 2010*".

Detecting Hyphenated Words and Space-separated Words

Sometimes, normally hyphenated words or phrases can occur as two separate words. But CA DataMinder does not treat hyphenated words and space-separated words as synonymous. Be aware of this distinction when defining trigger search text. Use a | logical OR operator to detect both hyphenated and space-separated occurrences of your key words or phrases. For example:

Search text	Matches	But does not match:
long term	long term	long-term or longterm
long-term	long-term or longterm	long term
longterm	long-term or longterm	long term
{long term} {long-term}	long term, long-term or longterm	

Full details are in the Search Text Syntax appendix.

More information:

[Search Text Syntax](#) (see page 383)

Far Eastern Characters

CA DataMinder supports Unicode character sets. For example, you can set up policy triggers to search the contents of a file for Japanese words or phrases. For details about setting up Unicode support, see the *Platform Deployment Guide*; search for 'unicode characters, general configuration'.

Which Files Can be Searched For Key Text?

Many user policy triggers enable you to search document contents for key text. If CA DataMinder detects this text, the trigger activates.

CA DataMinder can look inside many different document types, including the following:

HTML files

These are documents that can be viewed on the Web. CA DataMinder supports HTML 3.0 or earlier.

Microsoft Office documents

These include Word, Excel and PowerPoint files:

Word documents

These are typically .docx, .doc or .dot files. CA DataMinder can search files created with Word 97 or later, including .wbk backup files. Files must be unencrypted (that is, not password-protected) and uncompressed.

Excel spreadsheets

These are typically .xlsx, .xls or .xlw files. CA DataMinder can search spreadsheets created with Excel 97 or later. CA DataMinder can search workbooks, worksheets and charts; it does not search other spreadsheet elements such as macros or lookup tables. Files must be unencrypted (that is, not password-protected) and uncompressed.

PowerPoint presentations

These typically have a .pptx or .ppt extension. CA DataMinder can search presentations created with PowerPoint 97 or later. Files must be unencrypted (that is, not password-protected) and uncompressed.

Microsoft Project documents

These typically have an .mpp extension. CA DataMinder can search the text content of these files created with Microsoft Project 98 or later.

PDF files

CA DataMinder can search documents created with Acrobat 4.0 or later. It cannot search PDF files that have document security turned on (typically, this applies to files that are password-protected).

XML files

CA DataMinder can search text between XML tags, but not the XML tags themselves.

Zip files

These typically have a .zip extension, but can include any archive of one or more compressed files. These include files created with compression tools such as WinZip® and gzip. Policy settings let you specify a maximum depth of zip file nesting and a maximum size for decompressed zip files.

Rich text format files

These typically have an .rtf extension, but CA DataMinder can search text files with any file name or extension.

Text files

These typically have a .txt extension, but CA DataMinder can search text files with any file name or extension.

FrameMaker MIF files

Maker Interchange Format files are created from Adobe FrameMaker documents. They have a .mif extension. CA DataMinder can only search the text content of these files.

Which Triggers?

The following triggers allow you to define a list of files to be searched:

- **Email:** Attachments and Document Classifier triggers
- **Data At Rest:** All triggers
- **Data In Motion:** All triggers
- **Web pages:** File Upload and Document Classifier triggers

Searching Zip Files for Key Text

Applicable only if your license agreement supports zip file searching.

CA DataMinder can search the text content of documents archived inside a zip file. However, the compressed and recursive nature of zip files requires special handling in order to alleviate processing delays. You can optimize zip file handling by editing settings in the user policy.

Note: A zip file is any archive of one or more compressed files. These include files created with compression tools such as WinZip® and gzip.

Nested Zip Files

Zip files can contain nested zip files, and can even contain nested zip files which themselves contain further nested zip files! To recursively decompress, extract and search the content of documents archived inside these nested zip files can cause a performance slowdown.

To alleviate this problem, you can specify the maximum depth of nesting supported by CA DataMinder. To do this, you edit the Maximum Depth of Nested Zip Files and E-mails setting in the user policy System Settings folder.

For example, if you set a maximum depth of 2, CA DataMinder drills down two levels of nesting to analyze archived documents. In practice, this means it searches the text content of documents archived inside a zip file that is itself included in a master zip file. If CA DataMinder detects a further level of nesting, it does not search the documents archived inside this further zip file.

Note: This policy setting also covers emails embedded inside a master email.

Maximum Size for Decompressed Zip Files

When you decompress a zip file, the total size of all its archived documents can be very large. To prevent excessive processing delays and memory usage, you can define a maximum size for decompressed zip files. CA DataMinder can search the text content of documents in the zip file until it detects a document that would, when decompressed, take the cumulative total size of the decompressed zip file above this maximum size.

To set this maximum size, you edit the Maximum Size of Decompressed Zip Files setting in the user policy System Settings folder. For example, if you set a maximum size of 1,000 KB, CA DataMinder can search the text content of documents inside a zip file until it detects a document that, when decompressed, takes the cumulative total decompressed size of the zip file over 1,000 KB. CA DataMinder then disregards that document, plus any other archived documents not yet searched.

Searching Embedded Emails for Key Text

Emails can contain embedded messages, and can even contain embedded messages which themselves contain further embedded messages! To recursively decompress, extract and search the text content of these embedded emails can cause a performance slowdown.

To alleviate this problem, you can specify the maximum depth of nesting supported by CA DataMinder. To do this, edit the Maximum Depth of Nested Zip Files and E-mails setting in the user policy System Settings folder.

For example, if you set a maximum depth of 2, CA DataMinder drills down two levels of nesting to analyze embedded messages. In practice, this means it searches the text content of a message embedded inside a message that is itself embedded inside an email. If CA DataMinder detects a further level of nesting, it does not search the messages embedded inside this further embedded message.

Note: This policy setting also covers nested zip files.

Search Text Variables

When defining the key words or phrases that you want a trigger to detect, you can use variables to represent certain types of information. You can also use 'unknown text' variables to save as-yet-unknown text as a searchable attribute of a captured file, Web or email event.

A wide range of variables are available, providing great flexibility when defining your search text. For example, you can use the %DIGITS% variable to detect any sequence of digits such as a credit card number or telephone number. Other variables force the trigger to consider the context in which an item of text occurs. For example:

%+URL% unipraxis

This expression only matches against 'unipraxis' if it appears as part of a URL, such as in www.unipraxis.com.

Buy %number% units at %money% each

This expression matches phrases such as 'Buy 100 units at \$34.45 each' and 'Buy 2000 units at £20' each.

Note: You can also use 'search text' variables when defining Parameter 7 in a document classification.

More information:

[Search Text Syntax](#) (see page 383)

Setting a File Size Limit

You can specify a limit on the maximum size of files to be searched. To do this, you edit the Maximum Size of Files setting in the user policy System Settings folder.

Note: To ensure that files of any size are searched, set Maximum Size of Files to a value of zero.

Chapter 10: Protecting Emails

This section contains the following topics:

[Overview](#) (see page 146)

[Detecting Email Addresses](#) (see page 149)

[Webmails Detected by the NBA](#) (see page 153)

[Emails Encrypted with Voltage SecureMail](#) (see page 154)

[Forwarding Emails](#) (see page 154)

[Replies to Incoming E-mails](#) (see page 157)

[Modifying Recipient Fields](#) (see page 159)

[Integration With E-mail Servers](#) (see page 159)

[Disable E-mail Integration for Specific Sources](#) (see page 165)

[E-mails in Public Folders are excluded from Policy](#) (see page 166)

[Viruses and Captured E-mails](#) (see page 166)

Overview

Control triggers in the user policy enable you to block specified emails or simply warn the sender or recipient. For example, you can block emails sent with inappropriate content or you can warn users against sending emails to specific addresses. You can also silently monitor email traffic.

Blocking Emails

You can configure the user policy to block specific incoming emails.

You can quietly block an email so that the intended recipient is unaware that the email was blocked. Or you can replace the email body text with a predefined notification. In both cases, you can also send an automatic reply to the sender with an explanatory message.

You can also block outgoing emails. When outgoing emails are blocked, CA DataMinder displays a notification dialog. You define the message that appears in the dialog. You can define separate messages for each control trigger.

Warning Users

You can configure user policy to warn users when they try to send (or open) an unauthorized email. The warning dialog lets the user choose whether to continue or not:

- If the user cancels the warning, this generates a *heeded warning* event. In effect, the user accepts the warning and quits trying to send or open the email.
- If the user continues to send (or open) the email, this generates a *disregarded warning* event. CA DataMinder permits the user to send or open the email but it records the fact that the user disregarded the warning.

Categorizing Emails

You can configure user policy to categorize emails. Categories are defined in email triggers. Categorization can be either automatic or manual, depending on how the control triggers are configured and whether the email was detected by a client agent or server agent.

If you want users to categorize their own emails, you can configure a control action to display a notification dialog listing the available categories.

Quarantining Outgoing Emails

For outgoing emails, you can detect and quarantine emails that require urgent review. You can optionally notify the sender that this has happened. Reviewers can subsequently release the email from quarantine (sending it to its intended recipients) or reject it (the email is not sent).

Informing or Notifying Users

You can display an advisory dialog whenever CA DataMinder detects an email that may be significant. This is useful if, for example, you want to notify users when specified emails arrive in their Inbox or you want to inform senders that their email is missing a disclaimer.

Silent Monitoring

You can silently record each occurrence when an email triggers a control action, but without blocking the email or displaying a warning. The user is completely unaware that their email triggered a control event.

For example, a humorous but inoffensive email attachment is circulating within your organization and your bandwidth is suffering. Configuring your control actions to generate silent events lets you discreetly trace the source of these emails.

Capturing Emails

For any email that triggers a control action, you can fully capture the associated email or attachment.

Or you can simply capture details about the event. These details include the user name, when the trigger was activated, and so on.

Forwarding emails

You can forward any email that activates a control trigger to another address. For example, if a user disregards a warning and sends an unauthorized email, you can forward a copy to their manager. The manager then receives a notification email with the original email included as an attachment.

Exempting Emails

You can block or warn against unencrypted emails or emails without a digital signature, but exempt these emails if they are encrypted or digitally signed. To do this, you edit filter settings in each control trigger.

Alternatively, you can set up triggers to block encrypted or signed emails, but exempt non-encrypted or unsigned emails!

Automatic Replies to Incoming Emails

For any incoming email that triggers a control action, you can send an automatic reply to the sender. You choose what information is included in the reply. You can use automatic replies to notify the sender when their email has been blocked or when it generated a warning. Alternatively, you can use this feature to send an automatic acknowledgement to the sender.

More information:

[Notification Dialogs](#) (see page 347)

Chapter 11: Detecting Email Addresses

This section contains the following topics:

[Email Address Matching](#) (see page 149)

Email Address Matching

Email triggers allow you to define lists of included or excluded email addresses. You can also include display names in your address lists.

There are different formats for email addresses (for example, SMTP and X.400). Typically, you need lists of email addresses that [match all address formats](#) (see page 152). Alternatively, you can use format identifiers to [match specific address formats](#) (see page 153).

Display names

CA DataMinder automatically searches for email display names, so you can add items such as 'Spencer Rimmel' or '*Rimm*' to your list of included or excluded addresses.

Note: CA DataMinder interprets a space between address elements as an AND operator.

SMTP

SMTP is the most commonly used protocol for sending and receiving emails. Addresses use this format:

`spencer.rimmel@unipraxis.com`

To match against a specific organization, add this list item:

`*unipraxis.com`

To match against a specific person, add this list item:

`spencer.rimmel*`

Note: For incoming emails in Microsoft Outlook, SMTP addresses may be converted to EX addresses if the sender's address already exists in an Outlook address book. To ensure that policy triggers activate as expected, you may need to include both SMTP and EX versions in your list of included or excluded addresses, or define a list that matches all email address formats.

EX

This protocol is used internally by Microsoft Outlook. EX addresses take the following form:

```
/o=Unipraxis/ou=uk/cn=spencer/cn=rimmel
```

If you include EX addresses in a policy list, insert spaces between each address element (CA DataMinder interprets spaces as AND operators). This ensures the policy trigger always activates, regardless of how the email address elements are ordered.

If required, you can explicitly specify EX addresses to detect emails sent internally within your organization using Microsoft Outlook.

Examples

To match email addresses from a specific organization, add this list item:

```
/o=Unipraxis
```

To match email addresses for a specific sender or recipient, add this list item:

```
/cn=spencer /cn=rimmel
```

To match emails specifically sent using Outlook, add this list item:

```
ex: /o=Unipraxis /cn=spencer /cn=rimmel
```

Domino

This protocol is used internally by Domino. Domino addresses use this format:

```
cn=rimmel/ou=UK/o=unipraxis
```

If you include Domino addresses in a policy list, insert spaces between each address element (spaces are interpreted as AND operators). This ensures the policy trigger always activates, regardless of how the email address elements are ordered.

If required, you can explicitly specify Domino addresses to detect emails sent internally within your organization using Lotus Notes.

Examples

To match email addresses from a specific organization, add this list item:

```
/o=unipraxis
```

To match email addresses for a specific sender or recipient, add this list item:

```
/cn=spencer /cn=rimmel
```

To match emails specifically sent using Notes, add this list item:

```
notes: /o=Unipraxis /cn=spencer /cn=rimmel
```

Bloomberg alias addresses

These are alias addresses for participants in Bloomberg IM conversations or in Bloomberg messages embedded in EML emails that were by CA DataMinder utilities Cnv2email.exe or BB2email.exe. These alias addresses are stored as x-headers in the email and can be analyzed by CA DataMinder policy engines. Bloomberg alias addresses use this format:

BLP: /CN=99775533/O=222555

Where CN= identifies an individual user and O= is the Firm ID.

Note: Unlike other address formats where the identifier is optional, you must always include the Bloomberg identifier when defining a list of Bloomberg addresses.

Examples

To match email addresses from a specific organization, add this list item:

BLP: O=222555

To match email addresses for a specific sender or recipient, add this list item:

BLP: CN=99775533

X.400

X.400 is a widely-used protocol in Europe and Canada. X.400 email addresses use this format:

c=uk;a= ;p=Unipraxis;o=Exchange;s=rimmel;g=spencer

If you include X.400 addresses in a policy list, insert spaces between each address element (CA DataMinder interprets spaces as AND operators). This ensures that the policy trigger always activates, regardless of how the email address elements are ordered.

Examples

To match email addresses from a specific organization, add this list item:

p=Unipraxis

To match email addresses for a specific sender or recipient, add this list item:

s=rimmel; g=spencer

To specifically match x.400 emails, add this list item:

x400: s=rimmel; g=spencer

Internal emails

CA DataMinder uses the same methods of address matching to identify internal emails. That is, the guidelines above also apply when you define 'internal' address patterns in the user policy.

More information:

[Matching All Email Address Formats](#) (see page 152)

[Matching Specific Email Address Formats](#) (see page 153)

[Spaces in Email Addresses](#) (see page 153)

[Wildcards and Policy List Items](#) (see page 68)

Matching All Email Address Formats

Different email servers use different addressing protocols and consequently email addresses have different formats. But with careful planning, you can define lists of included or excluded email addresses that match against any targeted address, regardless of the email format used.

To define a 'universal' email address, enter the basic keywords such as a person's name and the Internet domain, separated by spaces and omitting any protocol-specific elements such as @ or p=.

For example, to match any emails sent to Spencer Rimmel of Unipraxis plc, add this item to your list of included email addresses:

rimmel unipraxis

This example matches all of the following formats because both keywords are present in each format:

- **SMTP:** spencer.rimmel@unipraxis.com
- **EX and Domino:** /o=unipraxis/ou=uk/cn=spencer/cn=rimmel
- **X.400:** c=uk;a= ;p=unipraxis;o=Exchange;s=rimmel;g=spencer

Note: CA DataMinder interprets a space between keywords as an AND operator.

More information:

[Copy and Import List Items](#) (see page 73)

[Spaces in Email Addresses](#) (see page 153)

Matching Specific Email Address Formats

Alternatively, you can specify particular address formats. For example, you may want to set up a trigger to detect emails sent from Bloomberg terminals. To specify particular address formats, you add identifiers to your address lists so that email triggers only detect specific address formats. The supported identifiers are:

ex:

notes:

BLP:

x400:

For example, add this item to an address list if you only want to detect Unipraxis emails sent using Domino:

notes: /o=unipraxis

Spaces in Email Addresses

For Included or Excluded lists of email addresses, CA DataMinder interprets spaces between keywords as an AND operator.

But for other policy lists such as lists of key phrases window titles or URLs, spaces are interpreted as literal characters, not as AND operators.

Webmails Detected by the NBA

The NBA can detect webmails sent from unrecognized addresses (such as `mysteryman@hotmail.com`) and pass these webmails to policy engines for processing.

Available control actions

The policy engines apply Outgoing Email triggers to these webmails. You can use these triggers to block, quarantine or categorize webmails. You can also set up CA DataMinder to send a blocking notification to the sender. See the *CA DataMinder Network Implementation Guide* for details.

However, the NBA does **not** support the Warn, Inform or Encryption options provided with email control actions.

More information:

[Applying Policy to Files Being Copied](#) (see page 185)

Emails Encrypted with Voltage SecureMail

You can configure CA DataMinder to detect, analyze, and apply policy to emails encrypted by Voltage SecureMail. After setting up SecureMail integration, you can apply Outgoing Email triggers to these encrypted emails as normal.

Which agents can detect SecureMail-encrypted emails?

The following agents can detect and apply policy to emails encrypted by Voltage SecureMail:

- Exchange server agent
- IIS SMTP server agent
- Milter MTA agent (for Sendmail and Postfix email servers)
- CA DataMinder Network (formerly known as the NBA). This agent can detect and apply policy to SMTP emails encrypted by SecureMail.

How do I set up SecureMail integration?

You must edit the registry on your policy engines, set a shared secret, and establish an SSL connection to the SecureMail web service.

Policy engines use the shared secret to establish secure connections to the Voltage SecureMail server. Full details are in the *Platform Deployment Guide*.

Forwarding Emails

Control actions allow you to forward incoming and outgoing e-mails. For example, you may want to forward suspicious e-mails to a manager for their approval or to a quarantine account.

In the email control action, edit the Forward Emails? and Forward To? settings. These settings determine when CA DataMinder forwards an email (for example, when the original email was blocked) and who it forwards the email to.

More information:

[Sending Forwarded Emails to Someone Else](#) (see page 155)

[Account Requirements for Forwarded E-mails](#) (see page 156)

[Forwarding E-mails to Multiple Addresses](#) (see page 157)

Sending Forwarded Emails to Someone Else

Control actions let you forward incoming and outgoing e-mails. For example, you may want to forward suspicious e-mails to a manager for their approval or to a quarantine account. If the manager then wants to send the e-mail to someone else, the method varies according to the type of e-mail system they use.

Lotus Notes

When you forward an e-mail in Notes, for example to a manager, it is included as a message thread in a notification e-mail. If the manager wants to send the e-mail to someone else, they can simply forward the notification e-mail in the normal way.

Microsoft Outlook

When you forward an e-mail in Outlook, for example to a manager, it is included as an attachment in a notification e-mail. If the manager then wants to send the forwarded e-mail to someone else (perhaps the e-mail was deemed benign so they want to return it to the intended recipient) they can:

- Forward the notification e-mail, with the original e-mail still included as an attachment.
- Open the attachment and forward the original e-mail to its intended recipient.

More information:

[Forwarding E-mails to Multiple Addresses](#) (see page 157)

Account Requirements for Forwarded E-mails

You specify the target account for forwarded e-mails in the user policy. The recipient account for forwarded e-mails has special requirements:

Do not send automatic replies from Out of Office

Do not configure Out of Office to send automatic replies to incoming messages. For example, if you choose to forward e-mails to a manager but this person turns on Out of Office when they go on holiday, the intended recipient of a forwarded e-mail will receive an automatic reply from Out of Office. This may cause confusion if the original incoming e-mail was blocked without notifying the intended recipient - that is, the Intervention setting is set to Block Quietly.

Correctly specify the recipient address

Important! This requirement applies particularly to incoming e-mail control actions.

Verify that you have specified the correct target account for forwarded e-mails. If you misspell part of the e-mail address, your e-mail server will be unable to deliver forwarded e-mails to this account and may send an 'Undeliverable' notification to the intended recipient. This is clearly undesirable in the case of incoming e-mails that were blocked without notifying the intended recipient (Block Quietly-see above).

The handling of undeliverable emails varies, according to the email system used by the forwarding machine:

Microsoft Outlook

If Outlook cannot deliver an e-mail, it sends an 'Undeliverable' notification to the intended recipient. This notification message includes a Send Again button that enables users to read the original e-mail. In this case, a user will be able to read the forwarded e-mail.

Lotus Notes

CA DataMinder configures the Notes delivery options so that delivery reports are turned off. This allows you to quietly block inappropriate incoming e-mails and forward them without any risk of alerting the intended recipient if the forwarding fails. (Delivery report inform intended recipients about a non-delivery and allow them to read the original e-mail.)

Note: These problems also occur if a forwarded e-mail cannot be delivered to the target address because, for example, there is a network problem or the e-mail server is down.

More information:

[Forwarding E-mails to Multiple Addresses](#) (see page 157)

Forwarding E-mails to Multiple Addresses

Control actions allow you to forward incoming and outgoing emails. For example, you may want to forward suspicious emails to a manager for their approval or to a quarantine account.

If required, you can configure the Forward To? setting in an email control action to forward an email to multiple addresses. Separate each address with a comma or semicolon:

`srimmel@unipraxis.com,fschaeffer@unipraxis.com`

`srimmel@unipraxis.com;fschaeffer@unipraxis.com`

Note: You can only forward emails to multiple addresses from CA DataMinder machines that use Lotus Notes.

Replies to Incoming E-mails

The control actions for incoming e-mails enable you to send an automatic reply. For example, you can send a reply to the sender, explaining that their e-mail was blocked and did not reach its intended recipient, or you can use this feature to send automatic acknowledgements to your customers.

To send automatic acknowledgements, you would set up a control trigger to activate when an incoming e-mail refers to, for example, one of your products. You could then configure the associated control action to send an automatic reply, perhaps thanking the customer for their interest. (To use the Reply feature in this way, you would set the Intervention action setting to 'None'.)

When you configure the reply message, you define the subject and body text and whether or not the original incoming e-mail is included as an attachment.

More information:

[Identifying which E-mail Triggered an Automatic Reply](#) (see page 158)

Identifying which E-mail Triggered an Automatic Reply

If you configure a user policy to send automatic replies, be aware that the reply does not explicitly identify the original e-mail that triggered the control action. If you choose not to attach the original e-mail to the reply, the sender may not know which of their e-mails the reply refers to. For this reason, we recommend two fixes. You can use them individually or together:

- **Fix 1** Always attach the original e-mail in any automatic reply. To do this, set the Attach Original? setting to True in the user policy.

Note: Use the Find feature to locate this setting.

- **Fix 2** Include the %subject% variable when you configure the Reply Subject setting. This setting defines the subject for the automatic reply. The %subject% variable appends the original e-mail's subject.

Example: If the subject of a blocked e-mail was 'Job Opportunities!' and you set the Reply Subject setting to:

This e-mail is a reply to: %subject%

Then the subject for the e-mail reply will be:

This e-mail is a reply to: Job Opportunities!

More information:

[Replies to Incoming E-mails](#) (see page 157)

[Find a Policy Folder or Setting](#) (see page 59)

Modifying Recipient Fields

Control actions allow you to move To or Cc recipients to the Bcc field on outgoing e-mails, to help ensure the e-mail complies with the regulations of your organization.

Note: These actions are only available for Outlook e-mails.

To modify recipient fields

1. Open the User Policy Editor and locate the Outgoing E-mail control action that you want to change.
2. Edit the Address Modification of Authorized E-mails setting. Choose one of the following options:

None

Leaves recipients exactly where they are in the To or Cc field.

Move external To/Cc addresses to the Bcc list

Moves all external recipients from the To and Cc fields to the Bcc field. An external recipient is any recipient not marked as 'internal'.

Move all To/Cc addresses to the Bcc list

Moves all recipients from the To and Cc fields to the Bcc field.

Note: If you choose to move all recipients or all external recipients, the e-mail event is marked accordingly. This information can then be seen when reviewing the event.

Integration With E-mail Servers

CA DataMinder can interrgate with email servers such as Exchange, Domino, IIS SMTP, Sendmail and Postfix. This allows CA DataMinder to monitor and control corporate email activity that would otherwise be missed by endpoint integration alone, including emails sent using BlackBerry handhelds, Microsoft Office Outlook Web Access or Notes Web Clients.

Server-side versus Client-side

CA DataMinder supports both client-side and server-side email integration. Specifically, it can integrate with Microsoft Outlook or Lotus Notes on client machines and with Microsoft Exchange, IIS SMTP, Domino, Sendmail and Postfix email servers. But there are two key differences between these email integration methods:

First and most important, the range of available control interventions is slightly more limited under server-side integration. Specifically:

- CA DataMinder can intervene by blocking an email and sending a notification message to the sender; or in the case of emails that generate warning or inform events, it can simply send a notification message to the sender. However, it cannot display warning dialogs that require user interaction (unlike under client-side integration, when CA DataMinder *can* display dialogs that require user interaction).
- With Microsoft Exchange server or IIS SMTP agents, CA DataMinder can also intervene by sending an interactive warning email to the sender. The user can then reply to the message to disregard the warning, or do nothing to automatically heed the warning and the agent sends or does not send the email accordingly. This is possible for emails that generated warning or inform events and requires specific configuration on the machine hosting the agent.

Second, under server-side integration CA DataMinder always applies triggers from the sender's perspective (that is, it applies triggers for outgoing emails). This approach avoids unnecessary duplication of analysis and processing. These triggers are defined in the sender's user policy or, if the sender is not a recognized CA DataMinder user, in the policies for the Unknown Internal Sender or External Sender. This contrasts with client-side integration where CA DataMinder can apply both incoming email triggers (defined in the recipient's policy) and outgoing email triggers (defined in the sender's policy).

Intervention Options and E-mail Server Agents

When a CA DataMinder server agent detects an e-mail that causes a control trigger to fire, the e-mail server sends a warning e-mail to the sender.

At the same time, the sender's user policy permits the full range of options for the Intervention setting. The consequences of each Intervention option when invoked by an email server agent are shown below:

Block quietly

Not supported.

Block with Notification

Blocks the e-mail and sends a notification email to the sender. The original e-mail is included as an attachment.

Warn

Allows the e-mail to be delivered and sends a notification email to the sender. The original e-mail is not included.

If interactive warnings are enabled, CA DataMinder retains the original e-mail and sends a warning email to the sender. The sender can choose to allow or disallow the original e-mail. The original e-mail is not released unless the user replies to the warning email.

Warn, user may designate as personal

Allows the e-mail to be delivered and sends a notification email to the sender. The original e-mail is not included.

This option is not supported if interactive warnings are enabled.

Quarantine quietly

Marks the e-mail for quarantine. The sender is unaware that the e-mail has not been sent.

Quarantine with notification

Marks the e-mail for quarantine and sends a notification email to the sender.

Inform

Allows the e-mail to be delivered and sends a notification email to the sender. The original e-mail is not included.

Notify

Not supported.

None

Allows the e-mail to be delivered.

More information:

[Automatic Notifications](#) (see page 162)

Automatic Notifications

If the Exchange, Domino or IIS SMTP server agent intercepts an e-mail that generates a blocking, warning or inform event, CA DataMinder automatically sends a notification e-mail to the sender. For these notification emails, you can configure the:

- **Sender.** In effect, you can define a 'global sender' for these emails. For example, you can specify that the From: field in such emails is always set to HR@Unipraxis.com.
- **Subject text.** You can specify different subject text for blockings, warning and inform emails.
- **Body text.** This is defined in the in the 'Message to Users' setting of the relevant control trigger. This setting supports a number of variables (such as %Keysting% or %Subject%) that you can use to customize the notification message based on the circumstances of the original email that caused a trigger to fire. For example:

"Your e-mail has been blocked. It refers to %Keysting% and such references violate corporate guidelines."

Note: For instructions on setting up notification emails, see the *Message Server Integration Guide*.

More information:

[Intervention Options and E-mail Server Agents](#) (see page 161)

[Interactive Warnings](#) (see page 163)

Interactive Warnings

If CA DataMinder intercepts an email transiting through Exchange Server or IIS SMTP and the email generates a warning or inform event, CA DataMinder can automatically send a notification or an interactive warning email to the sender.

If the sender replies to this warning promptly (that is, before the warning timeout expires), then their email is released and sent to its intended recipients. If they do not reply (or reply too late), then CA DataMinder deems that they have heeded the warning and the email is disposed of without being released. The warning timeout defaults to 4 hours. That is, a user has 4 hours to reply if they want to disregard the warning and send their email anyway. But this timeout is configurable.

Interactive Warnings and Followup Messages

The sender of an email can receive a warning and, if necessary, a follow-up message from the email server agent. The text content of these messages is configurable, by using template text files referenced in the registry

Warning message

This is the first message the user receives. It is sent automatically when the agent intercepts an email that has generated a warning or inform event. By default, the message has the user's original email attached and states that it has triggered one or more warnings. It lists the warnings and advises the sender that if they want the email to be sent, they must reply to the warning message.

'Unmatched response message'

This message is automatically sent when the user replies to the warning message, but the original email is no longer on the Exchange or IIS server. In this situation, the user's reply cannot be matched to the original email and so the email cannot be released and sent. Replies are matched to their corresponding emails by a unique ID in the Subject. The original email may no longer be on the Exchange or IIS server for any of the following reasons:

- The user replied too late and the warning 'autoheed' timeout expired. (This timeout is defined by WarningHeedTimeoutMins.)
- The user replied to the warning more than once. The first reply matches the original email and allows it to be sent, which in turn, removes it from the Exchange or IIS server. Any subsequent replies therefore cannot be matched.
- The maximum number of pending warnings was reached and the user was unable to reply to the warning message before it was autoheeded.
- (Exchange 2007 and 2010 server agents, IIS SMTP agent) The agent holding the pending email and the agent holding the response email (the reply from the user) cannot communicate.

Setting Up Interactive Warnings

The text content of the warning email is fully configurable. You define the text content by editing a message template stored on the email server. These message templates support a number of variables (such as %subject% or %to%) that you can use to customize the warning message based on the circumstances of the original email that caused a trigger to fire.

However, before you can roll out interactive warning emails across your organization, you need to set up your email server agents. For example, in addition to defining your message templates, you need to create Compliance Release mailboxes and configure the CA DataMinder agents to use these mailboxes. Full instructions are in the *Message Server Integration Guide*.

Disable E-mail Integration for Specific Sources

For each control trigger in any user or group policy, you can disable CA DataMinder integration with specific email applications or import sources. Messages arriving via any other source are exempted and cannot activate a control trigger. Integration can be disabled for any email control trigger.

To disable integration for a specific trigger

1. Open the User Policy Editor and locate the email control trigger that you want to change.
2. Edit the Which Email Sources? setting and choose which sources to target, for example, Microsoft Outlook.

Example: Capture imported emails and block emails sent through Exchange

In this example, you set up user policy to block unauthorized emails if they are sent through your Exchange server but to capture them, without the associated blocking event, when such emails are imported from an archive.

1. Set up a control trigger to block unauthorized emails transiting through your Exchange server:
 - a. In the User Policy Editor, locate the email control trigger that you want to use.
 - b. Edit the Which Email Sources? setting and select only the 'Microsoft Exchange Server (Mailbox)' option.

The trigger ignores imported emails and emails sent from other email applications.
 - c. Set any other trigger settings as required. For example, configure the trigger to only activate when it detects emails sent to members of the Research department.
 - d. Set up a control action to block and, if required, capture these emails.
2. Set up a capture trigger to capture all emails imported from, for example, PST files.
 - a. In the User Policy Editor, locate the email capture trigger that you want to use.
 - b. Edit the Which Email Sources? setting and select only the 'Archive File Importers' option.
 - c. Set up other trigger settings to ensure that all imported emails are captured.
3. Save the policy.

Note: You can also disable email integration completely, or for individual capture triggers. In addition, you can disable email integration when you install CA DataMinder, or you can specify that integration is disabled automatically if the CA DataMinder infrastructure fails to start.

More information:

[Data Lookup](#) (see page 293)

E-mails in Public Folders are excluded from Policy

The CA DataMinder Outlook client agent does not handle e-mails saved in Public Folders. This prevents triggers from activating unnecessarily to capture or block attempts to read e-mails in Public Folders.

Viruses and Captured E-mails

Important! If your virus scanners fail to prevent a virus attack, infected e-mails may be captured and saved in your CA DataMinder database.

If your organization suffers a virus attack, there is a risk that infected e-mails or attachments may be captured and saved in your CA DataMinder database. If this happens, you must delete any infected e-mails or attachments from all affected CA DataMinder databases (on the CMS plus any gateways or client machines that may also be at risk) as part of your cleanup operations after the attack.

Chapter 12: Encrypting Emails

CA DataMinder can insert 'encryption request' x-headers into unprotected outgoing emails. These x-headers can then be detected by third party encryption providers such as Voltage and PGP before they leave the corporate network.

First, you must specify which third party encryption provider you want to use. You do this in the user policy. Then you must set up your email triggers and control actions to detect and encrypt unencrypted emails.

This section contains the following topics:

[Specify the Encryption Providers](#) (see page 167)

[Set Up Encrypt Control Actions](#) (see page 171)

Specify the Encryption Providers

In the current release, CA DataMinder can support up to four encryption providers. PGP and Voltage SecureMail are supported by default and you can also add support for two further providers. However, an individual user policy must specify which one of these providers to use.

You specify the encryption providers in the user policy System Settings. In each case, you specify the provider's name, and the name and value of the x-header used to flag emails that require processing by a third-party encryption solution.

To set email encryption settings

1. In the User Policy Editor, navigate to the following folder:
System Settings, Email Encryption Settings
2. If you want to use:
 - PGP or Voltage to encrypt emails, go to step 5.
 - A different third party encryption provider, go to step 3.

3. Open a 'User Defined' Encryption Provider folder and edit these settings:

Provider Name

Enter the name of your third party encryption provider that you want to use (for example, 'Unipraxis Solutions')

X-header Name

Enter the x-header name that you agreed with your encryption provider (for example, x-unipraxis-msg').

X-header Value

If required, you can enter a value for the x-header (such as 'Encryption Request'). This value gets appended to the email x-header in this format:

x-unipraxis-msg: Encryption Request

4. Save the policy changes to ensure that the new encryption provider gets added to the list (see step 6).
5. Return to the System Settings, Email Encryption Settings folder.
6. In the Which Encryption Provider? setting, choose the provider you want to use.

X-header Requirements

Be aware that any x-headers generated from CA DataMinder user policies must adhere to the following requirements:

X-header names must start with X— or x—

x-header names must start with X— or x—. CA DataMinder specifically checks for 'x hyphen' smart tags when generating x-headers.

X-header names must be strong

This is crucial. When agreeing the x-header name with a third party, you must choose a 'strong' name. That is, choose a name that will not conflict with other x-headers. Specifically, avoid names that are generic or too short.

Notes and Domino users must also take care to choose x-header names that (when they have been stripped of the x— prefix) do not conflict with object names used internally by Domino.

An example of a strong x-header name is:

X-Unipraxis-MessageEncryptionRequest

Maximum length, x-header names and values

X-header **names** cannot be longer than 125 characters. Therefore, your smart tag name is similarly restricted. That is, the name you supply when editing the Smart Tags setting cannot be longer than 125 characters.

X-header **values** must not exceed 2,000 characters. X-header values are appended to the x-header name.

Although an x-header value is unlikely to be constrained by this limit, it may become more relevant in future CA DataMinder releases. For example, if a future release permits users to generate x-header values from tokens or variables (such as a 'distribution list' variable), this could potentially result in very long text strings.

Note: These x-header name and value limits are imposed by the technologies underlying the email systems (such as Outlook or Exchange). They are not inherent restrictions in the specification of Internet Mails.

X-headers cannot be added to encrypted or digitally signed emails

CA DataMinder Outlook endpoint agents cannot add x-headers to emails that have been encrypted or digitally signed.

Note: This limitation does not affect the Exchange server agent, though any policy triggers configured to detect email content may be unable to process encrypted emails anyway.

More information:

[X-header Limitation in Exchange 2003](#) (see page 170)

[X-Headers and Smart Tags](#) (see page 280)

Define Rule for Voltage SecureMail Gateway

If you use a Voltage SecureMail clientless solution (also known as 'SecureMail FlagSecure'), emails are not encrypted when they are sent but contain an x-header to indicate that encryption is required. Therefore you must define a rule on your SecureMail Gateway to encrypt the email.

Note: If you use a Voltage SecureMail end-to-end solution, emails are already encrypted before they leave the workstation or mobile device.

You *must* use 'x-voltage: encrypt'

To support CA DataMinder integration with SecureMail, you *must* define a SecureMail Gateway rule to detect the following x-header:

x-voltage: encrypt

This is the default x-header for SecureMail FlagSecure. *Do not specify a different x-header!*

Note: For details about configuring gateway rules, see the *Voltage SecureMail Management Console Administrator Guide*.

Why is this necessary?

CA DataMinder policy engines can only recognize 'x-voltage: encrypt' x-headers in SecureMail emails. They cannot recognize different x-headers.

CA DataMinder uses this x-header to mark SecureMail emails as 'Encrypted' when a user reviews these emails in the iConsole.

Note: If you use a different x-header, CA DataMinder still applies policy to the email. And the email is still encrypted by the SecureMail Gateway. However, CA DataMinder does not mark the email as 'Encrypted' in the iConsole.

X-header Limitation in Exchange 2003

Problems in Exchange 2003 cause the following x-header limitation for outgoing emails processed by a CA DataMinder Outlook endpoint agent and subsequently sent using Exchange.

Do not include periods in x-header names

If your x-header name includes a period character (such as X—Case.ID), Exchange 2003 will fail to insert the x-header into the email. In detail, although the Outlook endpoint agent successfully sets the appropriate email property, Exchange 2003 subsequently fails to convert this property to an x-header when this email is sent as an Internet Mail.

Note: This limitation has been fixed in Exchange 2007. Likewise, this limitation only applies to outgoing emails processed by the Outlook endpoint agent; it does not apply to emails processed by CA DataMinder Exchange or Domino server agents or the Notes endpoint agent.

Set Up Encrypt Control Actions

To set up an Encrypt control action

1. In the User Policy Editor, set up your Outgoing Email control triggers as required.
2. Set up your Outgoing Email control action. In particular, set the Intervention setting to one of the following:

Advise Encryption

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog to the email sender. The sender can choose one of the following:

- Encrypt their email (they must supply a password)
- Send the email unencrypted.
- Cancel the email.

For emails detected by a CA DataMinder email server agent, CA DataMinder can send a warning email back to the sender (providing server-side warnings are enabled). If the sender replies promptly, their original email is released and sent unencrypted. Otherwise it is not sent.

Enforce Encryption.

For emails detected by a CA DataMinder endpoint agent, CA DataMinder displays a warning dialog to the email sender. The sender can choose one of the following:

- Encrypt their email (they must supply a password)
- Cancel the email.

They cannot choose to send the email unencrypted.

For emails detected by a CA DataMinder email server agent, CA DataMinder can send a warning email back to the sender (providing server-side warnings are enabled). If the sender replies promptly, their original email is released and sent encrypted. Otherwise it is not sent. It cannot be sent unencrypted.

Important! If server-side interactive warnings are enabled, make sure that the message to users in the warning email clearly explains the consequences of replying and not replying! In particular, note the different reply handling for the Advise Encryption and Enforce Encryption options.

Chapter 13: Protecting Files Being Copied

You can use the Client File System Agent (CFSA), also known as 'Policy on Save', to control user attempts to copy files off the local hard disk. For example, the CFSA can monitor files being copied to removable storage devices (such as USB flash drives and SD cards), sync folders (such as DropBox), network locations, and writable CDs and DVDs. The CFSA can selectively block or allow a file and apply policy triggers based on a file's text content or properties. For example, it can force users to encrypt files being copied onto removable devices.

The CFSA can also scan the local hard disk and apply policy triggers based on a file's text content or properties. For example, it can categorize files based on their text content, and delete, replace or move unauthorized files.

This section contains the following topics:

[How Does CA DataMinder Protect Files on Removable Devices?](#) (see page 173)

[How Does CA DataMinder Protect Files in Network Folders?](#) (see page 178)

[How Does CA DataMinder Stop Users Burning Files to CD?](#) (see page 181)

[How Does the CFSA Protect Files in Sync Folders?](#) (see page 182)

[Applying Policy to Files Being Copied](#) (see page 185)

How Does CA DataMinder Protect Files on Removable Devices?

CA DataMinder can detect when a user tries to copy files to removable devices such as USB flash drives or SD cards.

Opening a file on a removable device

(Optional) When the CFSA detects a user trying to *open* a file on a prohibited device, it displays an Access Denied message. This message typically warns users that they are barred from saving file changes. You configure the Access Denied message in the user policy.

Note: A prohibited source is any removable device to which write access is denied. Write access may be denied by settings in the local machine policy or by Data In Motion triggers in the user's policy.

Copying a file to a removable device

When CA DataMinder detects a user trying to save a file to a removable device, it applies policy in the following sequence. The process is also summarized in the following [flow chart](#) (see page 176).

1. **CFSA checks whether the user is using a trusted application.**

Settings in the machine policy identify 'trusted applications'. If the user is using:

- A trusted application, the CFSA always allows the user to copy or save the file to a removable device. No further policy is applied.
- Any other application, the CFSA checks the handling for the removable device or network location (see step 2).

2. **CFSA checks the handling for the removable device.**

Settings in the machine policy define the 'handling' for removable devices. The available handling options are:

Allow write access

The user is allowed to copy files to this device.

Set to read only

The user is blocked from copying files to the device. That is, Write access to the device is disallowed.

Apply user policy

The CFSA checks whether the user is using a policy-enabled application to copy the file (that is, Windows Explorer or DOS).

You can also configure default handling for unrecognized devices and custom handling for 'special devices'.

3. **CFSA checks whether the user is using a policy-enabled application.**

These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the device is set to Read Only.

Warning! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

4. **CFSA applies Data In Motion triggers.**

Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author. Each trigger can also apply a further device filter to monitor specific removable devices.

If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file. You can also configure control actions to encrypt sensitive files being copied to a removable device (the user must supply a decryption password).

If no control trigger fires, the user is allowed to copy the file.

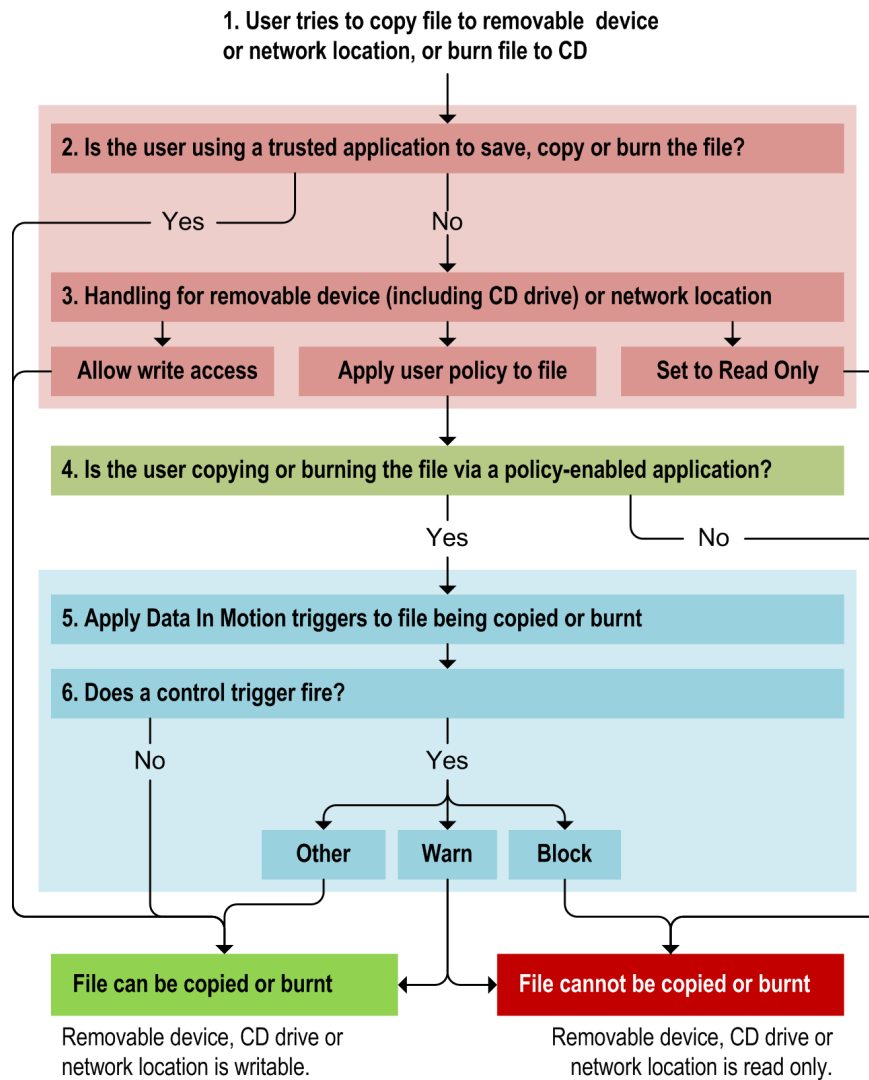
CFSA Flow Chart: Removable Devices, CD Drives, Network Folders

In the diagram below, a user tries to copy a file to a removable device or network location, or burn it to a CD (1). First, the CFSA checks whether the user is using a trusted application (2). If they are, it permits the file to be copied or burnt.

If the user is not using a trusted application, the CFSA checks the device, CD drive or location handling (3). If set to 'allow write access', file copying or burning is allowed; if it set to 'read only', the file is blocked.

Alternatively, if the handling is set to 'apply user policy', the CFSA checks whether a policy-enabled application is being used to copy or burn the file (4):

- If so, the CFSA applies policy triggers to the file (5). If a control trigger fires (6), this determines whether to block the file operation. If no control trigger fires, the file can be copied or burnt.
- If the user is not using a policy-enabled application, the file is blocked.



How Does CA DataMinder Protect Files in Network Folders?

CA DataMinder can detect when a user tries to copy files to network locations such as shared folders.

Opening a file from a prohibited network location

(Optional) When the CFSA detects a user trying to *open* a file from a prohibited network folder, it displays an Access Denied message. This message typically warns users that they are barred from saving file changes. You configure the Access Denied message in the user policy.

Note: A prohibited source is any network location to which write access is denied. Write access may be denied by settings in the local machine policy or by Data In Motion triggers in the user's policy.

Copying a file to a network location

When CA DataMinder detects a user trying to save a file to a network location, it applies policy in the following sequence. The process is also summarized in the previous [flow chart](#) (see page 176).

1. CFSA checks whether the user is using a trusted application.

Settings in the machine policy identify 'trusted applications'. If the user is using:

- A trusted application, the CFSA allows the user to copy or save the file. No further policy is applied.
- Any other application, the CFSA checks the handling for the network location (see step 2).

2. **CFSA checks the handling for the network location.**

Settings in the machine policy define the 'handling' for network locations. The available handling options are:

Allow write access

Users can always save files to this network location.

Set to read only

Users are blocked from saving files to this network location.

Apply user policy

The CFSA checks whether the user is using a policy-enabled application to copy the file (that is, Windows Explorer or DOS).

You can also configure custom handling for 'special locations'.

Note: When you specify the network locations that you want to monitor, always enter the UNC path. For example:

\\UX-FILESVR-01\New Project\Reports

If a path contains spaces, do not enclose it in quotes.

3. **CFSA checks whether the user is using a policy-enabled application.**

These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the target network folder is set to Read Only.

Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

4. **CFSA applies Data In Motion triggers.**

Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author.

If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file.

If no control trigger fires, the user is allowed to copy the file.

Note: The CFSA cannot encrypt files being copied to network locations. Do not use Encryption control actions to prevent unencrypted files being copied to shared locations on your network.

Local Drives Listed As Network Drives Over RDC

The CFSA can apply policy to local drives that have been added as network drives in a Remote Desktop Connection (RDC) session.

The Windows RDC feature allows users to use local disk drives in a remote session. For example, a user working from home connects to their office workstation using RDC. When the RDC session starts, the user can add their local C drive as a network drive on the remote workstation. This network drive represents a security risk, because the user can drag and drop sensitive files from their workstation onto their local C drive.

From a policy viewpoint, the CFSA handles these RDC network drives in the same way as other network locations. To apply policy to files being copied to this network drive in an RDC session, add one of the following values to the Special Locations List setting:

```
\\tsclient\C  
\\tsclient\D  
\\tsclient\*
```

These values apply policy to, respectively, the local C drive, local D drive, or all local drives mapped as network drives in an RDC session.

Find the Special Locations List setting in the following folder in the machine policy:
/Client File System Agent/Data in Use Protection/Network Locations folder.

How Does CA DataMinder Stop Users Burning Files to CD?

CA DataMinder can detect when a user tries to burn a file to CD or DVD.

The CFSA automatically recognizes writable CD and DVD drives and handles these drives in the same way as removable devices.

Note: In this section, the term 'CD drive' also refers to DVD drives.

Burning a file to CD or DVD

First, the CFSA applies machine policy in real time to block unauthorized file operations. It can also apply Data In Motion triggers to analyze the file being copied. The process is summarized below and in the previous [flow chart](#) (see page 176).

1. CFSA checks whether the user is using a trusted application.

Settings in the machine policy identify 'trusted applications'. If the user is using:

- A trusted application, the CFSA allows the user to burn the file. No further policy is applied.
- Any other application, the CFSA checks the handling for the CD drive (see step 2).

2. CFSA checks the handling for the CD drive.

Settings in the machine policy define the 'handling' for writable CD drives. The available handling options are:

Allow write access

Users can always save files to this CD drive.

Set to read only

Users are blocked from saving files to this CD drive.

Apply user policy

The CFSA checks whether the user is using a policy-enabled application to copy the file (that is, Windows Explorer or DOS).

Note: When configuring the CFSA machine policy settings, you do not need to add writable CD drives to the Treat These Drives As Removable setting. The CFSA automatically treats these drives as removable and applies the device handling to them. For example, to prevent any files being burnt to CD, you can set the device handling to 'Set to read only'.

3. CFSA checks whether the user is using a policy-enabled application.

These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the CD drive is set to Read Only.

Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

4. CFSA applies Data In Motion triggers.

Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author. Each trigger can also apply a further device filter to monitor specific removable devices.

If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file.

If no control trigger fires, the user is allowed to burn the file.

Note: 'Encrypt' control actions are not supported. You cannot encrypt files being burned to CD.

How Does the CFSA Protect Files in Sync Folders?

CA DataMinder can detect when a user tries to drag or copy files into sync folders such as DropBox. It also detects when a user tries to upload a file to a file sync website such as DropBox.com.

Note: When you drag and drop a file into a sync folder in Windows Explorer, CA DataMinder copies the file instead of moving it.

File Sync Methods: Application versus Web site

File sync providers such as DropBox typically provide two sync methods:

- Users can install a Windows Explorer plug-in on their workstation. This plug-in is the 'file sync application' (see below). The user launches Windows Explorer and drags or copies the file that they want to share into the sync folder.

The CFSA can protect files being synced using this method.

- Users can log in to file sync web site (such as DropBox.com) and upload the file that they want to share into the sync folder.

The Client Network Agent (CNA) can protect files being synced using this method.

CA DataMinder provides Data In Motion protection for both file sync methods.

How Does CA DataMinder Protect Files Being Copied to Sync Folders?

1. CFSA checks machine policy for file sync applications.

(Not applicable to files being uploaded to a file sync website.)

First, the CFSA checks the local machine policy in real time to determine whether the file sync application is under policy control. By default, CA DataMinder can apply policy to files being synced to:

- Box
- DropBox
- Google Drive
- Microsoft SkyDrive

If the file sync application is *not* under policy control, CA DataMinder allows the file to be synced.

But if the file sync application *is* under policy control, CA DataMinder checks whether the user is using a policy-enabled application to copy the file.

2. CFSA checks whether the user is using a policy-enabled application.

These are applications that the CFSA can integrate with to apply user policy. If a user copies a file using a policy-enabled application *and* the target handling is set to 'Apply user policy', the CFSA applies Data In Motion triggers to the file.

If the application is *not* policy-enabled, the CFSA blocks the file. From the user's viewpoint, the sync folder is set to Read Only.

Important! The only policy-enabled applications recognized by the CFSA in the current release are: Windows Explorer (including drag and drop copying); DOS commands such as copy and xcopy; Wordpad.exe; and Notepad.exe.

3. **CA DataMinder applies Data In Motion triggers.**

The file sync method affects which CA DataMinder endpoint agent handles the policy analysis.

Using a file sync application plug-in

If an employee uses a Windows Explorer plug-in to copy files to a sync folder, the *CFSA* detects the sync operation and applies Data In Motion triggers.

Verify that the Client File System Agent is selected in the Which Files Sources? setting.

Using a file sync web site

If an employee uploads a file to a file sync web site, the *Client Network Agent* detects the sync operation and applies Data In Motion triggers.

Verify that the Client Network Agent for File is selected in the Which Files Sources? setting.

In both cases, DIM triggers can analyze the text content to detect key phrases or check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to detect file attributes such as size, date created, date last modified, and the file author.

4. **CA DataMinder applies Data In Motion control actions.**

If a trigger fires, you can configure control actions to block the file sync operation.

Alternatively, if the user is using a file sync application, you can set up triggers to warn the user. Or you can allow the file sync operation but categorize or encrypt the file (the user must supply a decryption password).

If no control trigger fires, the user is allowed to copy or upload the file.

Applying Policy to Files Being Copied

To protect files being to removable devices, network locations, CD or DVD, or sync folders, you must edit the local machine policy and the user policy.

Note: Details about key policy settings are provided in the following topics.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. Edit the machine policy. For example:
 - a. Expand the Machine Administration branch.
 - b. Right-click the CMS and click Edit Common Client Policy.
3. Browse to the following folders:

Data In Use Protection folder

Find this folder in the Client File System Agent folder.

Edit the Included Files and Excluded Files settings.

Removable Devices folder

Find this folder in the Data In Use Protection folder.

Edit settings in this folder to protect files files being copied to removable devices and CD drives.

Network Locations folder

Find this folder in the Data In Use Protection folder.

Edit settings in this folder to protect files files being copied to network locations.

File Sync Providers folder

Find this folder in the Data In Use Protection folder.

Edit settings in this folder to protect files files being copied to sync folders.

Policy Engine folder

(Optional) For performance reasons, you may need to amend settings in this folder. Only edit these settings if instructed to do so by CA technical staff.

4. Save the machine policy changes.
5. Edit the user policy.
 - a. Expand the User Administration branch.
 - b. Right-click a user or group and click Edit Policy.
6. Edit the **Data In Motion** triggers.

7. Edit the **Data In Motion** control actions.
8. (Optional) Edit settings in the **Access Denied Message** folder.
Find this folder in the Extensions > Client File System Agent folder.
9. Save the user policy changes.

Configure the Local Machine Policy

To configure the CFSA, edit settings in the Client File System Agent folder of the machine policy on each endpoint computer. We recommend that you edit the Common Client Policy. You may also need to adjust settings in the Policy Engine folder.

The key machine policy settings are described in the following sections.

Data In Use Protection folder

Find this folder in the Client File System Agent folder.

Edit the Included Files and Excluded Files settings.

You also need to edit settings in the following subfolders:

Removable Devices folder

Find this folder in the Data In Use Protection folder.

Edit settings in this folder to protect files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

Network Locations folder

Find this folder in the Data In Use Protection folder.

Edit settings in this folder to protect files being copied to network locations. These network locations can include drives mapped over a Remote Desktop Connection (RDC).

File Sync Providers folder

Find this folder in the Data In Use Protection folder.

Edit settings in this folder to protect files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

Policy Engine folder

(Optional) For performance reasons, you may need to amend settings in this folder. Only edit these settings if instructed to do so by CA technical staff.

Data In Use Protection Folder

Settings in this folder determine which files are monitored. This folder also includes the following subfolders: Removable Devices, Network Locations, and File Sync Providers.

In each case, you can define a list of trusted applications. If the user is using a trusted application, CA DataMinder always allows them to save or copy files to these targets.

Included Files; Excluded Files

These settings determine which files to monitor. By default, the Included setting lists all the common document types such as '*.doc' and '*.ppt'. No files are excluded by default, but if required you can use the Excluded list to omit specific file types such as .mp3 or .log files.

Note: The Excluded list takes precedence if there is a conflict. For example, you can include all spreadsheets (*.xls') but exclude specific files such as 'Holiday_Form.xls'.

More information:

[Removable Devices Folder](#) (see page 188)

[Network Locations Folder](#) (see page 190)

[File Sync Providers Folder](#) (see page 192)

Removable Devices Folder

Edit settings in this folder to protect files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

This folder contains the following settings:

Trusted Application List

These are applications that are exempted from CFSA control. That is, users are permitted to copy files to removable devices using these applications. For example, you may not need to monitor an in-house system application that always encrypts files when saving.

Add the applications you want to exempt from the CFSA. You must supply the executable or process name, such as Winword.exe.

Note: Trusted applications override any device filters. That is, a user can copy a file directly from a trusted application to a removable device, even if the handling for that device blocks such copy operations or applies policy to the file content.

Isass.exe always included

By default, Isass.exe is always included in this list—see the ‘trusted application’ definition in CFSA terminology.

Anti Virus Programs

If a client machine is protected by an anti-virus program, we recommend that you add the process name to the Trusted Application List. For example, add InoRt.exe if it is protected by CA eTrust Threat Management.

Treat These Drives As Removable

This setting instructs the CFSA to handle a fixed drive as if it were a removable drive. For example, some external hard disks declare themselves as being a fixed drive when in fact they are easily removable. Ordinarily, the CFSA would not apply policy to files being saved to these drives. To close this loophole, you can explicitly identify these drives as removable.

In the Treat These Drives As Removable setting, you can add the drive letter or the disk drive name (also called the ‘volume identifier’) set by the manufacturer. Drive letters must include a colon (such as D:). Disk drive names are shown in Windows Device Manager (such as IC25N020ATC504).

Note: The CFSA automatically treats writable CD and DVD drives as removable drives.

Default Handling

The handling determines whether a device is writable or read only. This setting controls attempts to copy files to unlisted devices (that is, any device not in the Special Device List). The available actions are exactly the same as the handling for special devices (see below).

Note: If no special devices are listed, the default handling is applied to all devices.

Special Device List

This is a list of removable devices that require specific handling by the CFSA. For example, you identify the devices you want the CFSA to control or the ones you want it to ignore.

In the Special Device List setting, type the names of the devices that require special handling. You can use ? and * wildcards if required. If a device name contains spaces, you do not need to enclose it in quotes.

Where can I find device names?

Device names are shown in the Windows Device Manager applet. You can also see them in Windows Explorer. When you view the properties of a removable drive, the device name is listed in the Hardware tab of the Properties dialog.

You can also check device names in Windows Device Manager. Note that Device Manager automatically appends 'USB Device' to device names. You must omit this appended text when you specify the device name in the machine policy or user policy. For example, if the Device Manager lists 'Unipraxis DataStick 2.0 USB Device', enter this in the policy as 'Unipraxis DataStick 2.0'.

Handling for Special Devices

This setting determines how the CFSA handles attempts by a user to copy files to any removable device included in the Special Device List. The available actions are:

Allow write access

The user is allowed to copy files to listed devices. Policy is not applied.

Read only

The user is not allowed to copy files to listed devices (unless they are using a trusted application). Policy is not applied.

Apply User Policy To File

If the user attempts to copy a file to a listed device using:

- A policy-enabled application, policy is applied to the file using Data In Motion triggers.
- A trusted application, copy operations are always permitted. Policy is not applied to the file.
- Any other application, the copy operation is blocked; that is, the device is set to read only.

Network Locations Folder

This folder contains the following settings:

Trusted Application List

These are applications that are exempted from CFSA control. That is, users can save files to any network location if they are using a trusted application.

For example, you may not need to monitor an in-house system application that always encrypts files when saving. By default, lsass.exe is always included in this list—see the *trusted application* definition in 'CFSA Terminology'.

In the Trusted Application List setting, add the applications you want to exempt from the CFSA. You must supply the executable or process name, such as Winword.exe.

Note: Trusted applications override any network location filters. Users can save files directly from a trusted application to any network location.

Default Handling

This setting determines how the agent handles attempts to copy files to unlisted network locations (that is, any not listed in Special Locations List). The available actions are exactly the same as for special locations (see below).

Note: If no special locations are listed, the default handling is applied to all network locations.

Special Locations List

This setting is a list of network locations that require specific handling by the CFSA. You can either list the locations you want the CFSA to control or the ones you want it to ignore.

When you specify a network location, you must supply the UNC path. This path must use a fully qualified domain name (FQDN). For example:

\\UX-FILESVR-01.UNIPRAXIS.COM\My Project\Reports

Local Drives Listed As Network Drives Over RDC

The CFSA can apply policy to drives mapped over a Remote Desktop Connection (RDC).

The Windows RDC feature allows users to use local disk drives in a remote session. For example, a user working from home connects to their office workstation using RDC. When the RDC session starts, the user can add their local C drive as a network drive on the remote workstation. This network drive represents a security risk, because the user can drag and drop sensitive files from their workstation onto their local C drive.

To apply policy to files being copied to this network drive in an RDC session, add one of the following values to Special Locations List:

\\tsclient\C

\\tsclient\D

\\tsclient*

These values apply policy to, respectively, the local C drive, local D drive, or all local drives mapped as network drives in an RDC session.

Wildcards

When you specify a UNC path, you can use wildcards to specify the share name, folder name and file name. But do *not* use wildcards to specify the server. For example, this path is allowed::

\\UX-FILESVR-01.UNIPRAXIS.COM\My Project*\Report*

But this path is *not* allowed:

\\UX-FILESVR-*.UNIPRAXIS.COM\My Project*\Report*

Spaces

If a UNC path contains spaces, you do not need to enclose it in quotes.

Handling of Special Locations

This setting determines how the CFSA handles attempts to copy files to a network location listed in Special Locations. The available actions are:

Allow write access

The user is allowed to copy files to special locations. Policy is not applied.

Read only

The user is not allowed to copy files to special network locations (unless they are using a trusted application).

Apply User Policy To File

If the user attempts to copy a file to a special location using:

- A policy-enabled application, policy is applied to the file using Data In Motion triggers.
- A trusted application, copy operations are always permitted. Policy is not applied to the file.
- Any other application, the copy operation is blocked; that is, the location is set to read only.

File Sync Providers Folder

Edit settings in this folder to protect files being copied to sync folders. These settings determine whether a user is allowed to copy files using a file sync application such as Dropbox.

In particular, these settings determine whether the file sync application is under policy control. If the file sync application *is* under policy control, CA DataMinder applies Data In Motion triggers to analyze the file being synced.

Note: These settings do *not* apply to files being uploaded to file sync websites.

Trusted Application List

This setting grants the listed application access to file sync folders on the local computer. For example, you may want to add virus scanners to this list. You can also use this setting to extend data protection to other file sync applications.

Type the executable names of any additional file sync applications that you want to include under CFSA control. You must also add the sync folder for the new file sync application to the Additional Sync Folders setting.

Which File Sync Applications?

This setting lists the default set of file sync applications supported by the CFSA. Select the file sync applications that you want the CFSA to monitor.

Additional Sync Folders

Use this setting to specify any additional sync folders that you want the CFSA to monitor.

You can use system variables such as %windir% when specifying folder paths.

Policy Engine Folder

For performance reasons, you may need to amend these settings in the Policy Engines folder. You must only edit these settings if instructed to do so by CA technical staff:

Maximum Number of Concurrent Operations

Defines the maximum number of files that can be processed simultaneously by a policy engine.

Deadlock Detection Timeout (seconds)

Specifies how long a worker thread must be inactive while processing an event before the policy engine considers the thread to have stalled.

Configure the User Policy

You must edit your user policies to complete the CFSA configuration.

Files being copied to removable devices, network locations, writable CD drives

To protect these files, edit the Data In Motion triggers and control actions.

You must also configure the Access Denied Message. Users see this message when a file copy operation is blocked.

Files being synced to sync folders

To protect these files, edit Data In Motion triggers and control actions.

Data In Motion Triggers

Data In Motion triggers include general settings that let you specify which types of data you want the CFSA, CPSA, or Client Network Agent to detect. This section focuses on the key Data In Motion settings for the CFSA.

Which File Sources?

In each Data In Motion trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents.

Verify that the following sources are selected:

- Client File System Agent

You *must* select this agent if you want to analyze files being copied to removable devices, network locations, or sync folders in Windows Explorer.

- Client Network Agent for File

(Optional) Select this agent if you also want to analyze files being copied to file sync websites such as DropBox.com.

Which Targets?

(Not applicable to file sync operations and files copied to network folders. To specify network locations, edit the Top Level File Lists settings.)

Note: Depending on the Which File Sources? setting, the Targets settings can specify lists of removable devices, printer names, network folders, URLs, or writable CD drives.

For the CFSA, you can specify lists of included or excluded devices. These lists are similar to the Special Device List settings in machine policy.

Type the names of the devices that you want to include or exclude. Use ? and * wildcards if required. If a device name contains spaces, you do not need to enclose it in quotes.

If you set up the trigger to use:

- Included removable devices, the trigger only fires if a user tries to copy a file to a listed device using a 'policy-enabled application'.
- Excluded removable devices, these devices are exempted from control by the CFSA. But attempts to copy files to any other (unlisted) removable devices, via a policy-enabled application, *will* fire the trigger.

Where can I find device names?

Device names are shown in the Windows Device Manager applet. You can also see them in Windows Explorer. When you view the properties of a removable drive, the device name is listed in the Hardware tab of the Properties dialog.

You can also check device names in Windows Device Manager. Note that Device Manager automatically appends 'USB Device' to device names. You must omit this appended text when you specify the device name in the machine policy or user policy. For example, if the Device Manager lists 'Unipraxis DataStick 2.0 USB Device', enter this in the policy as 'Unipraxis DataStick 2.0'.

Top Level File Lists (including network locations)

All Data In Motion triggers include Top Level File Lists. Use these lists to detect normal files or zip files, or files in network locations.

Edit these lists to identify the names of files that you want to apply policy to. For example, you can specify:

- * to analyze all files
- *.docx to analyze all .docx files
- A list of specific .zip files to analyze.

For each trigger, choose whether to use an Included, Excluded or Ignored file list.

Network Locations

You also use this setting to specify UNC network paths. This path must use a fully qualified domain name (FQDN). Use a wildcard to detect all files in the specified folder. For example:

\\UX-FILESVR-01\New Project\Reports*.*

If a path contains spaces, you do not need to enclose it in quotes.

Individual/Embedded File List

If required, Data In Motion triggers can look for files contained within a zip file or embedded in a master file. To do this, edit the Individual/Embedded File Lists. For each trigger, you can choose to use an Included or Excluded file list.

Using these lists in conjunction with the Top Level File Lists, you can feasibly search all .zip files for a specific file. For example, set Included Top Level Names to *.zip and Included Individual/Embedded File Names to *.doc to search for all .doc files contained within .zip files.

Intervention

In each Data In Motion control action, the Intervention setting determines how the CFSA handles files being copied to removable devices, network locations, or sync folders. The available options include Block, Warn, Inform, Categorize and Encrypt (the user must supply a decryption password).

Note: The CFSA cannot encrypt files being copied to network locations.

Access Denied Message Subfolder

If required, you can display a message when a user opens a file from a prohibited source. This message typically warns users that they are barred from saving changes to the file. For example, when you edit the Frequency setting in the \Access Denied Message subfolder, you can set the message to display once only when a user first opens a file from a prohibited source.

Note: A prohibited source is any removable device or network location to which write access is denied. Write access may be denied by settings in the local machine policy or by Data In Motion triggers in the user's policy.

Find the Access Denied Message subfolder in the \Extensions\Client File System Agent folder. This subfolder contains the following settings:

Title, Message

Use Title and Message settings to provide a notification message for users, explaining that they will be unable to save changes to the current file.

Frequency

The Frequency setting determines how often this message is shown. You can set the message to never display, or to display:

- Once per login: A user only sees the message once in a Windows session. This happens the first time they open a file from a prohibited device or network location.
- Once per volume mount: A user sees the message if they plug in a prohibited device such as a USB drive and then open a file from that device. The message is only shown the first time they open a file from that device.
- Once per application: A user sees the message when they open a file from a prohibited source. The message is only shown once per application per Windows session. For example, the message is shown if they open a Microsoft Word document stored on a prohibited USB device. If they then restart Word and open the document again, the message is not shown.
- Once per application instance: A user sees the message each time they open a file from a prohibited source. As above, the message is shown if they open a Microsoft Word document stored on a prohibited USB device. But now if they restart Word and open the document once more, the message is shown again.

Specifying File Names and Types

Each Data At Rest and Data In Motion trigger includes two types of file lists:

- **Top Level File Names.** These settings let you check for names of 'normal' files or zip files.
- **Individual or Embedded File Names.** These settings can detect named files contained within a zip file or embedded in a master file.

Both types of setting can detect specific files or types of file, including scanned files, files being copied to a removable device or network location, imported files and files entering or leaving the corporate network. Together, these settings allow you to specify different handling for unauthorized files depending on where the file was found.

Included, Excluded and Ignored file lists

For both the Top Level File Names setting and Individual or Embedded File Names setting, you can use an Included list or an Excluded list. For Top Level File Names settings, you can also use an Ignored list.

Example File Names

For example, you can specify:

- '*' to detect all files in a folder.
- '*.docx' to detect all Microsoft Word files.
- '%allarchives%' to search all archive file types. The %allarchive% variable refers to file types listed in the Archive File Extensions setting (see below).
- A list of specific .zip files. (This is only appropriate for Top Level File Names settings.)

Example: Conditional File Handling

If the CFSA detects the file Q1targets.docx saved in a public folder on your network, you may want to simply delete the file. But if it is found inside a zip file that contains other important data, you may prefer to simply move the zip file to safe location. To set this up in the user policy, you use two Data At Rest triggers and two control actions:

- The first trigger includes Q1targets.docx in the Top Level File Names setting and invokes a DoD Delete control action.
- The second trigger includes '*.zip' in the Top Level File Names setting and Q1targets.docx in the Individual or Embedded File Names setting. It invokes a 'Copy and Delete' control action, effectively moving the parent zip file to a new location.

Defining archive files

You can specify which file types CA DataMinder will recognize as 'archive' files. To do this, edit Archive File Extensions setting in the user policy. Find this setting in the \System Settings folder. Specify the archive file types, such as *.zip, *.pst, or *.gz.

More information:

[Files Entering or Leaving the Corporate Network](#) (see page 232)

What File Data is Captured?

The Capture File Details? setting in each Data In Motion and Data At Rest capture action determines what information is captured. You can choose to capture:

File attributes only

CA DataMinder captures various file attributes but not the file itself, such as: the file name and path; the host machine; the created and last modified dates; the document title and author (if available); plus other details in XML format.

Attributes and file data

CA DataMinder captures the attributes described above plus the file itself.

None

You can optionally set up the capture action to not capture any file details. This option is provided for testing purposes.

Chapter 14: Encrypting Files Being Copied

This section contains the following topics:

[Overview](#) (see page 201)

[Specify Which Removable Devices To Monitor](#) (see page 202)

[Configure Encrypt Actions in the User Policy](#) (see page 204)

[Educate Your Users About the Encryption Utility](#) (see page 205)

[CA DataMinder Cannot Encrypt Files Copied to Network Locations](#) (see page 207)

Overview

Data In Motion triggers in each user policy support Encrypt control actions. The Encrypt control actions can protect sensitive files when an employee copies them to removable devices or file sync folders.

For example, you can add Encrypt options to the policy of an employee who needs to take sensitive files home to work on them over the weekend. In this example, CA DataMinder encrypts these files when the employee copies them onto a removable device for the journey home. When the employee gets home, they run an encryption utility on the removable device to decrypt the files onto their home computer. In the morning, the process is reversed. When the employee copies the updated files from their home computer back onto the removable device, CA DataMinder re-encrypts the files. Finally, when the employee arrives back at the office, they run the same encryption utility again to decrypt the files and copy them from the USB device back onto their office computer.

In technical terms, the CA DataMinder Client File System Agent (CFSA) detects a file being copied and invokes Data In Motion triggers. If a trigger fires, an Encrypt control action gets applied to the file. A resulting advisory dialog then instructs the employee to protect the file by supplying a password that CA DataMinder uses to encrypt and decrypt the file.

To use this feature:

1. Edit the machine policy on your CA DataMinder endpoint computers.
2. Configure Data In Motion triggers to apply Encrypt actions to sensitive files.
3. Educate your users so that they know how to use the CA DataMinder encryption utility when copying files.

These steps are described in the following sections.

Note: The CFSA cannot encrypt files being copied to network locations.

Specify Which Removable Devices To Monitor

Before you set up policy triggers to force encryption of sensitive files, you must configure the CFSA.

To configure the CFSA, edit settings in the Client File System Agent folder of the machine policy on each endpoint computer machine. We recommend that you edit the Common Client Policy.

The key machine policy settings are described below.

Data In Use Protection folder

Find this folder in the Client File System Agent folder.

Edit the Included Files and Excluded Files settings.

You also need to edit settings in the following subfolders:

Removable Devices

Edit settings in this folder to protect files being copied to removable devices such as USB drives. These devices can also include SD cards and writable CD or DVD drives.

To ensure that copied files get encrypted, set the device handling to 'Apply User Policy'. If an employee uses a policy-enabled application to copy a file, the Apply User Policy option causes the CFSA to apply Data In Motion triggers to the file. If the application is not policy-enabled, the CFSA blocks the file from being copied.

You can also configure default handling for unrecognized devices and custom handling for 'special devices'.

File Sync Providers

Edit settings in this folder to protect files being copied to sync folders. These settings determine whether a user is allowed to copy files using a file sync application such as Dropbox.

To ensure that a synced file gets encrypted, verify that the file sync application is included in the Trusted Application List. This enables the CFSA to control the file sync application. In particular, it allows the CFSA to apply Data In Motion triggers to the synced file.

If the file sync application is not under CFSA control, CFSA blocks the file from being copied. In particular, these settings determine whether the file sync application is under policy control. If the file sync application *is* under policy control, CA DataMinder applies Data In Motion triggers to analyze the file being synced.

Note: Full instructions for configuring the CFSA are in the *Endpoint Integration Guide*. Search for 'Client File System Agent'.

Exempt PGP® Portable Devices

Files copied to a PGP Portable device are stored in a 'secure container' (a virtual disk drive on the device). You can set up user policies to exempt these devices from CA DataMinder encryption control.

To exempt PGP portable devices

1. In the Common Client machine policy, navigate to the following folder:
Client File System Agent, Data In Use Protection, Removable Devices
2. In the Special Device List setting, add the following new item:
PGP Portable

This ensures that CA DataMinder recognizes any PGP Portable device and does not apply policy to files being copied onto those devices.

Configure Encrypt Actions in the User Policy

You must configure the Data In Motion control triggers and actions to encrypt sensitive files being copied.

To set up an Encrypt control action

1. Edit the required user policies.
 - a. In the Administration console, expand the User Administration branch.
 - b. Browse to the user group whose policy you want to edit.
 - c. Right-click the user group and choose Edit Policy.
2. In the User Policy Editor, go to this folder:
Control, Data In Motion, Control Triggers
3. Edit your trigger settings as required. For example, you can specify search text to detect prohibited words or phrases in files being copied. Pay particular attention to these settings:

Which File Sources?

Verify that that this setting includes the Client File System Agent.

Use Content Agents for Files?

Specify whether to use content agents to detect files that you have previously fingerprinted.

Which Targets?

((Not applicable to file sync operations.) These settings allow you to target or exempt specific removable devices.

4. Go to this folder:
Control, Data In Motion, Control Actions
5. Set up your control action as required. In particular, set the Intervention setting to one of the following:

Advise Encryption

CA DataMinder displays an advisory message. The user can then choose to encrypt the copied file (they must supply a password) or they can copy the file unencrypted. Or they can cancel the copy operation.

Enforce Encryption.

CA DataMinder displays an advisory message. The user must supply a password to encrypt the file, or they can cancel the copy operation. They cannot copy the file unencrypted.

6. Save the user policy changes.

Educate Your Users About the Encryption Utility

When you roll out the CA DataMinder Encrypt feature across your organization, educate your users about how to encrypt and, critically, how to decrypt sensitive files. Your users must be familiar with the CA DataMinder encryption utility, CADLPEnc.exe.

Briefly, when a user copies a file to a removable device or sync folder, CA DataMinder prompts them for a password. CA DataMinder uses this password to encrypt the file before it is copied. To retrieve and decrypt the file, the user must run CADLPEnc.exe and re-enter the password that they used to encrypt the file.

Note: CADLPEnc.exe is copied with the file to the removable device or sync folder.

Example: Encrypting and decrypting a file on a removable device

Consider a user who wants to take sensitive files home to work on them over the weekend. From the user's viewpoint, there are four stages:

1. Before the user leaves the office, they must encrypt and copy a file onto a USB device.
2. When the user gets home, they must decrypt and copy the file onto their home computer.
3. Before the user leaves home and returns to the office, they must re-encrypt and copy the file back onto their USB device.
4. When they get back into the office, they must decrypt the file and copy it onto their home computer.

Before the user leaves the office

The user tries to copy an unprotected file (such as MyReport.docx) onto a USB device.

1. CA DataMinder displays an advisory message and prompts them for a password.



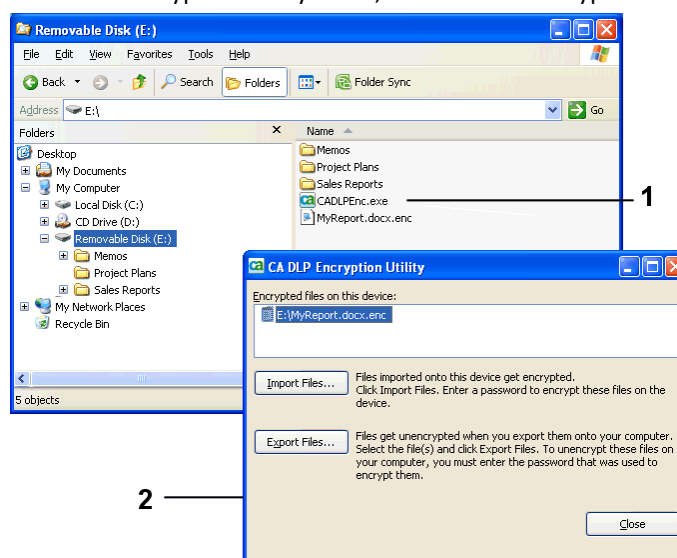
Encryption Advisory Dialog

2. CA DataMinder uses this password to save an encrypted version of the file onto the USB device. (The file is stored with an .enc suffix, such as MyReport.docx.enc.)
3. CA DataMinder copies the encryption utility, CADLPenc.exe, onto the USB device.

When the user gets home

The user must use the encryption utility to copy their file from the USB device onto their home computer.

1. The user runs the encryption utility, CADLPenc.exe. This utility is in the root of their USB device.
2. When the encryption utility starts, it lists all the encrypted files on the USB device.



1 Encryption utility, CADLPenc.exe, stored on removable device. **2** Encryption utility screen display.

3. The user selects the file they want and clicks Export Files.
4. The user chooses a target folder on their home computer.
5. CA DataMinder prompts for the password that they used to encrypt the file when it was copied onto the USB device.
6. CA DataMinder decrypts the file and copies it to the home computer.

Important! The user *must* use the encryption utility to copy the file from the USB device onto their home computer. If the user drags the file directly from the USB device onto the home computer, the file remains encrypted and is unusable!

Before the user leaves home and returns to the office

After the user has finished working on the file at home, they must encrypt and copy it back onto the USB drive:

1. The user runs the encryption utility on their USB drive.
2. The user clicks Import Files.
3. The user selects the file they want to copy from their home computer onto the USB device.
4. The encryption utility displays an advisory message and prompts the user for a password.
5. CA DataMinder uses this password to save an encrypted version of the file back onto the USB drive.

Note: The user does not have to enter the same password as before.

When the users gets back to the office

The procedure for getting the file off the USB device is exactly the same as the procedure when they get home.

1. The user runs the encryption utility from the root of their USB device.
2. When the encryption utility starts, it lists all the encrypted files on the USB device.
3. The user selects the file they want and clicks Export Files.
4. The user chooses a target folder on their office computer.
5. CA DataMinder prompts for the password that they used to encrypt the file when it was copied onto the USB device.
6. CA DataMinder decrypts the file and copies it to the office computer.

CA DataMinder Cannot Encrypt Files Copied to Network Locations

Note: The CFSA cannot encrypt files being copied to network locations.

The Intervention setting in Data In Motion control actions includes Advise Encryption and Enforce Encryption options. But these options are only intended to control unencrypted files being copied to USB devices. Do *not* use these options to encrypt files being copied to shared locations on your network.

Chapter 15: Detecting Fingerprinted Files

This section summarizes how to edit user policies to support Content Registration, also known as fingerprinting. You can set up triggers to use content agents. These agents can quickly recognize sensitive documents that have already been fingerprinted. If a user tries to copy, send or print them, or if CA DataMinder detects them during a file scan, the trigger fires and CA DataMinder can then apply appropriate policy controls.

For full details about creating and managing content agents, see the *Platform Deployment Guide*.

This section contains the following topics:

[About Content Registration \(Fingerprinting\)](#) (see page 210)

[Fingerprinting Components](#) (see page 210)

[Set Up Triggers to Detect Fingerprinted Files](#) (see page 212)

[Search for Fingerprinted Documents](#) (see page 213)

About Content Registration (Fingerprinting)

The Content Registration feature in CA DataMinder, also known as fingerprinting, enables you to take 'fingerprints' of sensitive documents that you want to protect. In effect, you can register the content of these documents so that they can be quickly recognized if a user tries to copy or send them or when CA DataMinder runs a file scan. CA DataMinder can then apply appropriate policy controls.

Fingerprinting is simple to roll out and does not require complex changes to your user policies. Instead of defining complex document classifications in the user policy, you can register the content of the files you want to protect.

Fingerprinting is also the best way to protect documents with highly specialized text content, such as source code, and files with little text content. For example, you can fingerprint CAD drawings, graphics saved in a spreadsheet, and multimedia files.

These fingerprints represent unique document signatures and are made available to CA DataMinder policy engines and endpoint agents. When CA DataMinder analyzes a file, it can quickly determine whether the file matches a known fingerprint and apply policy controls to that file. For example, it can block a fingerprinted document from being sent as an email attachment or copied to a USB device. It can even detect if a document or email contains extracts of text copied from a protected file.

Notes

- The ability to detect text extracts copied from a fingerprinted document is provided by Text Detection content agents.
- Content agents cannot reliably detect spreadsheets or printed files.

Fingerprinting Components

Fingerprinting in CA DataMinder relies on content agents, content indexes and specialized policy triggers.

Content agents

Each *content agent* has a list of protected files. These are files stored on your network whose content has already been scanned and fingerprinted. You can have as many content agents as you need. For example, you may have separate agents to fingerprint documents owned by the Finance and HR teams.

Create your content agents before you roll out fingerprinting across your CA DataMinder enterprise. For details about creating content agents, see the *Platform Deployment Guide* or the Administration console online help.

Note: The Content Registration feature uses File Scanning Agent technology to scan files and generate fingerprints.

Content indexes

A *content index* is a list of fingerprints for all the files protected by an individual content agent. You must manually build the index after creating a content agent. You must then publish the index to the CMS to make the content agent available to your policy engines and endpoint agents.

If the list of files protected by a content agent changes, you must rebuild and republish it. If you build an index again, it contains the fingerprints for the original list of protected files plus the fingerprints of any new or modified files. This means that the rebuilt index can contain fingerprints for both new and old versions of the same file. To eliminate multiple versions of the same file from the index, purge and rebuild the index.

If the file list changes are substantial, or if you remove a document from the protected files list, we recommend that you purge the index and then rebuild and republish it.

To build an index, CA DataMinder runs a specialized FSA scanning job.

Content agent triggers

A *content agent trigger* uses content agents to identify protected files. When the trigger analyzes a file (for example, an email attachment), it generates a digital signature, or fingerprint, for that file. The trigger then compares that fingerprint with lists of known fingerprints. If the fingerprints match, a policy trigger fires. You must set up your user policies to use content agent triggers before your fingerprinted files are fully protected.

Set Up Triggers to Detect Fingerprinted Files

To enable CA DataMinder to detect fingerprinted files, you need to edit triggers in your user policies. Specifically, you need to assign content agents to specific triggers and ensure that these triggers have distinctive names and, typically, an appropriate policy class.

After setting up your content agents and building the content indexes, you must assign the agents to triggers in your user policies. These triggers fire when they detect a file that matches a fingerprint in the content agent's index.

You also need to give these triggers distinctive names and, typically, an appropriate policy class. This enables reviewers to easily search for fingerprinted files captured or blocked by CA DataMinder.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. Expand the User Administration branch.
3. Right-click a user or group and choose Edit Policy.
4. In the User Policy Editor, select the trigger you want.

For email triggers, you can only assign content agents to a Content Agent trigger.

For Data In Motion and Data At Rest triggers, you can assign content agents to any trigger.

5. (Data In Motion triggers and Data At Rest triggers only) Edit the Use Content Agents For Files? trigger setting. Set this to 'Use content agents to analyze text content'.
6. Edit the Which Content Agents? trigger setting and add the content agents that you want to associate with this trigger.
7. Edit the Trigger Name and Policy Class settings as required.
8. Reviewers will search for 'fingerprint events' using these trigger names and policy classes.

Search for Fingerprinted Documents

You can use the iConsole to search for fingerprinted files detected by CA DataMinder. You need to filter your searches either by trigger name, (specifying the content agent triggers that detected the files) or by policy class (specifying the class assigned to these triggers).

To search for fingerprinted files

1. In the iConsole, edit the properties of the search that you want to run.
2. Go to the Incidents tab of the Search Properties screen.
3. Do one of the following:
 - In the Trigger Name field, choose the relevant trigger.
 - In the Policy Name field, choose the policy class associated with the relevant content agent.

Note: Only the standard CA DataMinder searches enable you to filter your search by trigger name or policy class.

Chapter 16: Controlling What Users Can Print

This section contains the following topics:

[Overview](#) (see page 215)

[When Do Triggers Activate?](#) (see page 216)

[Apply Policy Triggers to Printed Files](#) (see page 219)

Overview

A policy administrator can use the Client Print System Agent (CPSA) to control what information users are allowed to print. You can apply policy triggers when users try to print a file or document and you can also disable the Print Screen button on their keyboard.

The CPSA, or print agent, allows you to closely control the use of printers in your organization:

- If a user presses the Print Screen button, the print agent checks the user policy to determine whether the button is disabled.
- Alternatively, if a user attempts to print a document from an application (for example, by choosing File, Print), the print agent checks which application the user is using. If this is an 'ignored application', the user is allowed to print the document. For any other application, the print agent applies Data in Motion triggers.

First, these triggers check whether the printer itself is excluded from policy control. If so, the print job is allowed to continue. Otherwise, the trigger examines the file's properties and text content. The results of this policy processing determine whether the print agent blocks or allows the print job.

Notes

- For full details about deploying the CPSA and the required changes to user policies and machine policies, see the *Endpoint Integration Guide*.
- The CPSA is also known as *Policy on Print* or *PoP*.

When Do Triggers Activate?

The CPSA process is summarized below and in the following [flow chart](#) (see page 217).

1. (Optional) CPSA checks whether the user is using a trusted application.

First, the CPSA checks which application the user is using. If this is:

- If this is an 'ignored application' as defined in the registry, the CPSA allows the print job and no policy triggers are applied.
- If the application is not listed in the registry, the CPSA does apply Data In Motion triggers to the file or document

2. CPSA applies Data In Motion triggers.

Data In Motion triggers activate when the CPSA detects print jobs that match the specified criteria. For example, you can set up triggers to monitor (or exempt) specific printers on your network. You identify printers by their name, for example, 'HP Color LaserJet 4650 PCL 6 1st Floor'.

When a file is sent to a printer, triggers can detect specific file names and file formats (such as Microsoft Word documents). They can analyze the text content to detect the key phrases or to check whether the file matches a particular document classification. They can also use XML Attribute data lookup commands to file attributes such as size, date created, date last modified, and the file author.

Finally, you can configure triggers to block or allow the print job or to display a warning.

More information:

[Apply Policy Triggers to Printed Files](#) (see page 219)

[Do Not Specify File Names](#) (see page 220)

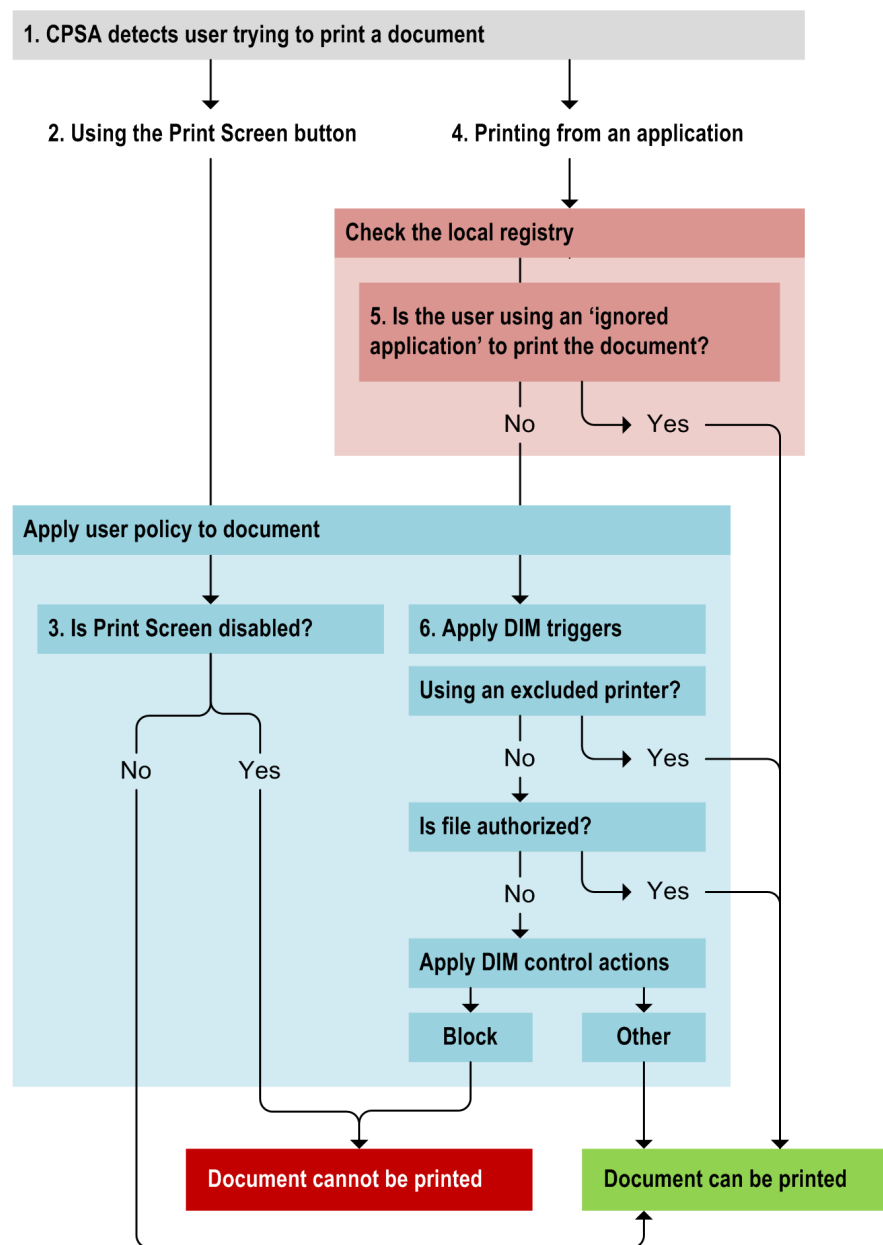
[XML Attribute Lookup Syntax](#) (see page 307)

CPSA Flow Chart

In the diagram below, a user tries to print a file (1). First, the CPSA checks whether the user is printing from an application or is using the Print Screen button.

- If the user is using the Print Screen button to send the screen contents to a printer (2), the CPSA applies user policy to the print request to determine whether or not the Print Screen button is disabled (2).
- If printing from an application (4), the CPSA checks the registry to see whether the application is exempt from policy control (5). If so, the CPSA allows the file to be printed. If not, it applies Data In Motion policy triggers (6).

These triggers first check if an authorized printer is being used. If so, the CPSA allows the file to be printed. If not, the file's properties and text content are analyzed. If the file is not authorized, a control action determines whether to allow the print operation. If the file *is* authorized, the print operation is allowed.



Apply Policy Triggers to Printed Files

To control what users can print, you must edit Data In Motion triggers in the user policy.

Note: Details about key policy settings are provided in the following topics.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. Edit the user policy.
 - a. Expand the User Administration branch.
 - b. Right-click a user or group and click Edit Policy.
3. Edit the Data In Motion triggers.

You also need to set the Intervention option in the Data In Motion control actions.

4. (Optional) Disable the Print Screen button.
5. Save the user policy changes.

More information:

[Specifying Printer Names](#) (see page 219)

[Do Not Specify File Names](#) (see page 220)

[Disable Print Screen Button](#) (see page 221)

[What Data is Captured?](#) (see page 222)

Specifying Printer Names

This section focuses on the key Data In Motion settings for the CPSA.

Which File Sources?

In each Data In Motion trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents. Verify that the following source is selected:

- Client Print System Agent

You *must* select this agent if you want to analyze files being sent to a printer.

Which Targets?

Note: Depending on the Which File Sources? setting, the Targets settings can specify lists of removable devices, printer names, network folders, URLs, or writable CD drives.

For the CPSA, you can specify lists of included or excluded printers. Type the names of the printers that you want to include or exclude. Use ? and * wildcards if required. If a printer name contains spaces, you do not need to enclose it in quotes.

If you set up the trigger to use:

- Included printers, the trigger only fires if a user tries to send a document to a listed printer.
- Excluded printers, these printers are exempted from control by the CPSA. Attempts to send documents to any other (unlisted) printer will cause the trigger to fire.

About printer names

The printer name typically comprises the printer model plus customized location details. For example, 'HP Color LaserJet 4650 PCL 6 1st Floor'. We recommend you enter the exact printer name. You can also use ? and * wildcards, for example, to specify all printers by a specific manufacturer.

Where can I find printer names?

Printer names are shown in the Windows Printers and Faxes applet. You can also check printer names in Windows Explorer; when you view the properties of a printer, its name is listed in the General tab of the Properties dialog.

Top Level File Names

Do not specify file names when you set up Data In Motion triggers for print events. The concept of a file name is not valid for CA DataMinder print events. For example, a user can print a single page from an unsaved (and unnamed) document. Do not change the default value of the setting when configuring print events.

Intervention

In each Data In Motion control action, the Intervention setting determines how the CPSA handles print jobs. The available options include Block, Warn, Inform, and Categorize.

Do Not Specify File Names

Do not specify file names when you set up Data In Motion triggers for print events. The concept of a file name is *not* valid for CA DataMinder print events. For example, a user can print a single page from an unsaved (and unnamed) document.

Therefore, do *not* change the default value of the Top Level File Names setting when configuring print events. This setting is included in each Data In Motion trigger.

More information:

[Apply Policy Triggers to Printed Files](#) (see page 219)

[Add Data Lookup Commands to Control Triggers](#) (see page 295)

Disable Print Screen Button

Users may attempt use the Print Screen button to circumvent the CPSA. You can configure CA DataMinder to disable the Print Screen button to prevent circumvention.

Note the following:

- No print event is generated when the CPSA blocks a Print Screen operation. Data In Motion triggers do not activate and CA DataMinder does not save details of these blockings in the CMS database.
- You cannot configure the Disable Print Screen feature. That is, you cannot set up the CPSA so that Print Screen is only disabled if it detects specific files, printers or applications.

When the user presses the disabled Print Screen button on their keyboard, CA DataMinder can optionally display a 'Print Screen Denied' warning message.

To disable the Print Screen button

1. Go to the \System Settings folder of the user policy.
2. Set the Disable Print Screen setting to True.

To configure a Print Screen Denied message

If required, you can display a message to alert or inform users that the Print Screen button is disabled.

1. Go to the \Extensions folder of the user policy.
2. Edit the settings in the \Print Screen Denied Message subfolder.
3. Specify the message content.

Example: "The Print Screen function is blocked. For assistance, contact your network administrator."

4. Specify the display frequency of the message. The available options for the Frequency setting are:

Never

The user never sees the message.

Once per login

The user sees the message once. This happens the first time they press the Print Screen button in a new Windows login session.

Always

The user sees the message every time they press the Print Screen button.

More information:

[Overview](#) (see page 215)

[Apply Policy Triggers to Printed Files](#) (see page 219)

What Data is Captured?

Set the Capture File Details? setting in each Data In Motion and Data At Rest capture action to determine what file information you want to capture.

File attributes only

Specifies that CA DataMinder captures various file attributes, but not the file itself. Attributes include the file name and path; the host machine; the created and last modified dates; the document title and author (if available); plus other details in XML format.

Attributes and file data

Specifies that CA DataMinder captures file attributes plus the file content.

None

Specifies that CA DataMinder does not capture any file details. This option is provided for testing purposes.

Chapter 17: Stopping Data Leaks to the Cloud

More information:

[About the Client Network Agent](#) (see page 223)

[How Does CA DataMinder Stop Data Leaking To the Cloud?](#) (see page 225)

[Applying Policy to HTTP Activity](#) (see page 226)

About the Client Network Agent

You can use the Client Network Agent (or 'network agent') to control web activity on endpoint computers. Specifically, the network agent can monitor HTTP requests. This activity includes attempts to post files and comments to web sites or to submit form data. It can also monitor attempts to check in files to SharePoint libraries.

Which browsers and applications are monitored by default?

By default, the network agent is configured to monitor web activity for most common browsers and Microsoft Office applications:

- Microsoft Internet Explorer
- Mozilla Firefox
- Opera
- Google Chrome
- SeaMonkey
- Safari
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

These browsers and applications are specified in the machine policy settings for the Client Network Agent.

How does the network agent differ from the Internet Explorer agent?

In previous versions of CA DataMinder, the Internet Explorer agent could only apply policy to web activity in Internet Explorer browsers. It applied Web triggers and could apply the full range of control actions, including Warn actions.

The network agent can apply policy to network activity in any browser and applies Data In Motion triggers. It does not support Warn control actions. Also, Data In Motion triggers offer greater file detection capabilities and also support Data Lookup commands.

Note: Unlike the Internet Explorer agent, the network agent cannot apply policy to file downloads.

How does the network agent differ from the CA DataMinder Network?

The CA DataMinder Network (NBA) operates at the network boundary and monitors outbound and inbound traffic. It runs on a dedicated Bivio hardware device or a dedicated Linux server. The NBA can also monitor traffic sent using multiple protocols, including SMTP and FTP. In particular, the NBA is able to differentiate webmails and apply Outgoing Email triggers.

The client network agent runs on users' workstations and monitors outbound network activity. Also, in the current release it can only monitor HTTP traffic.

How Does CA DataMinder Stop Data Leaking To the Cloud?

CA DataMinder can detect when a user submits data (files, comments, forms) to a web site.

1. **(Optional) Network agent checks whether the user is using an excluded application or browser.**

Settings in the machine policy can identify 'excluded' applications. If the user is using:

- An excluded application, the network agent ignores any HTTP activity. The user is allowed to submit data to a web site.
- Any other application, the network agent applies Data In Motion triggers to the data submission (see step 2).

2. **Network agent applies Data In Motion triggers.**

Data in Motion triggers can analyze data submitted to web sites. They can analyze the text content to detect key phrases or to check whether a submitted file matches a particular document classification. They can use XML Attribute data lookup commands to file attributes such as size, date created, date last modified, and the file author. Each trigger can also apply a further device filter to monitor specific removable devices.

If a trigger fires, you can configure control actions to block or categorize the data submission.

If no control trigger fires, the user is allowed to submit the data.

Applying Policy to HTTP Activity

To control HTTP activity, you must edit Data In Motion triggers in the user policy.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. (Optional) Edit the machine policy.
 - a. Browse to the Client Network Agent folder.
 - b. Edit the application lists.
3. Edit the user policy.
 - a. Expand the User Administration branch.
 - b. Right-click a user or group and click Edit Policy.
 - c. Edit the Data In Motion triggers.
 - d. Edit the Data In Motion control actions.
4. Save the user policy changes.

More information:

[Configure the Local Machine Policy](#) (see page 227)

[Configure the User Policy](#) (see page 228)

Configure the Local Machine Policy

(Optional)

If required, you can configure the network agent to ignore network activity in specific applications or browsers. You specify the applications and browsers in the machine policy. We recommend that you edit the Common Client Policy. The key settings are in the following folder:

Client Network Agent folder

This folder contains the Applications settings. If required, you can edit these settings to set which applications are exempt from or included in policy control. (By default, the network agent monitors common web browsers and Microsoft Office applications.)

Important! Be aware that the network agent is not suitable for monitoring Office Communicator traffic! See the note below.

Which Application List?

This setting specifies whether the network agent uses an Included or Excluded list of applications. By default, the network agent uses the Included list which contains a predefined set of default applications.

Included Applications

If you specify the Included list, the network agent only monitors the included applications for network activity. By default, this list includes most [common browsers and Microsoft Office applications](#) (see page 223).

Note: Before making any changes, review the applications that the network agent will monitor. For example, applications such as Windows Update Agent do not permit their network traffic to be intercepted and may be adversely affected.

Excluded Applications

If you specify the Excluded list, the network agent monitors all applications except those on the Excluded list. The network agent ignores network activity in excluded applications and browsers. Such activity is exempt from policy control.

For example, you may want to exempt Microsoft Word when it is used to check in or check out documents from a SharePoint site.

Note: By default, the following applications and services are *excluded* from policy control. You cannot override these defaults.

- Microsoft Office Communicator
- Windows services
- CA DataMinder

Configure the User Policy

To complete the network agent deployment, you must edit Data In Motion triggers and control actions in the user policy.

These triggers include settings that let you specify which types of document or data submission you want the network agent to detect. This section focuses on the key Data In Motion settings for the network agent.

Which File Sources?

In each Data In Motion trigger, this setting instructs the trigger to analyze files or documents captured by various CA DataMinder agents. Verify that the following agent is selected:

- Client Network Agent for File

You *must* select this agent if you want to analyze data submitted to web sites, including files being uploaded to file sync websites such as DropBox.com.

Which Targets?

Note: Depending on the Which File Sources? setting, the Targets settings can specify lists of removable devices, printer names, network folders, URLs, or writable CD drives.

Use the Targets settings to define URLs that you want to monitor or exempt. You can specify lists of included or excluded URLs.

Type the URLs that you want to include or exclude. Use ? and * wildcards if required. If you set up the trigger to use:

- Included URLs, the trigger only fires if a user tries to submit data to a URL on the Included list. For example, add `www.facebook.com` to the Included list.
- Excluded URLs, these URLs are exempted from control by the network agent. But attempts to submit data to any other (unlisted) URL *will* fire the trigger.

Top Level File Lists

All Data In Motion triggers include Top Level File Lists. Use these lists to detect normal files or zip files, or files in network locations.

Edit these lists to identify the names of files that you want to apply policy to. For example, you can specify:

- * to analyze all files
- *.docx to analyze all .docx files
- A list of specific .zip files to analyze.

For each trigger, choose whether to use an Included, Excluded or Ignored file list.

Individual/Embedded File List

If required, Data In Motion triggers can look for files contained within a zip file or embedded in a master file. To do this, edit the Individual/Embedded File Lists. For each trigger, you can choose to use an Included or Excluded file list.

Using these lists in conjunction with the Top Level File Lists, you can feasibly search all .zip files for a specific file. For example, set Included Top Level Names to *.zip and Included Individual/Embedded File Names to *.doc to search for all .doc files contained within .zip files.

Intervention

In each Data In Motion control action, the Intervention setting determines how the network agent handles data submissions to web sites. The key supported options are Block and Categorize. The Block option prevents the user from submitting data or uploading a file.

Note: The network agent also supports None and No Further Actions intervention options.

Chapter 18: Protecting Data at the Network Boundary

This section summarizes how CA DataMinder can apply policy to data submitted to web sites.

This section contains the following topics:

[Files Entering or Leaving the Corporate Network](#) (see page 232)

[Detecting URLs in Traffic Crossing the Network Boundary](#) (see page 233)

Files Entering or Leaving the Corporate Network

CA DataMinder can protect files entering or leaving your corporate network. These files include FTP file transfers, files sent as attachments to web mails or IM conversations, and files uploaded to or downloaded from web sites, and files copied during RDC sessions. CA DataMinder uses the following protection methods:

NBA applies filters to block communications directly

You can configure NBA network filters and application filters to block data packets directly. The filters use criteria such as the source or destination machine IP address or the protocol being used. For full details, see the *CA DataMinder Network Implementation Guide*.

CA DataMinder applies Data in Motion triggers to files captured by the NBA

The NBA can pass reassembled files to policy engines for processing. The policy engines apply Data In Motion triggers to files detected by the NBA.

Data in Motion triggers can analyze the text content to detect key phrases or to check whether the file matches a particular document classification. They can use XML Attribute data lookup commands to file attributes such as size, date created, date last modified, and the file author.

If a trigger fires, you can configure control actions to block or allow the file operation, or to categorize the file.

If no control trigger fires, the file is allowed to continue.

Note: For files captured by the NBA, CA DataMinder does not support the Warn, Inform, or Encrypt control actions.

CA DataMinder applies Data In Motion triggers to files copied over RDC

The CA DataMinder Client File System Agent (CFSA) can apply Data In Motion triggers to files being copied off a remote computer and onto a local drive in a Remote Desktop Connection (RDC) session.

For example, the CFSA can block a user from copying files from an office workstation to their home computer during an RDC session. See the reference below for details.

More information:

[Local Drives Listed As Network Drives Over RDC](#) (see page 180)

Local Drives Listed As Network Drives Over RDC

The CFSA can apply policy to local drives that have been added as network drives in a Remote Desktop Connection (RDC) session.

The Windows RDC feature allows users to use local disk drives in a remote session. For example, a user working from home connects to their office workstation using RDC. When the RDC session starts, the user can add their local C drive as a network drive on the remote workstation. This network drive represents a security risk, because the user can drag and drop sensitive files from their workstation onto their local C drive.

From a policy viewpoint, the CFSA handles these RDC network drives in the same way as other network locations. To apply policy to files being copied to this network drive in an RDC session, add one of the following values to the Special Locations List setting:

```
\\tsclient\C  
\\tsclient\D  
\\tsclient\*
```

These values apply policy to, respectively, the local C drive, local D drive, or all local drives mapped as network drives in an RDC session.

Find the Special Locations List setting in the following folder in the machine policy:
/Client File System Agent/Data in Use Protection/Network Locations folder.

Detecting URLs in Traffic Crossing the Network Boundary

You can use the NBA to apply policy to network traffic originating from specific URLs. For example, you may want to capture all Facebook traffic, but only capture traffic from other URLs if the communication breaches your corporate regulations.

Note: Network events can include file uploads, comments posted to a web site, and page requests submitted to a web server.

How does CA DataMinder Detect URLs?

1. When the NBA analyzes files crossing the network boundary, the NBA stores URL details with the event metadata.

For HTTPGET, HTTPPOST, and HTTPURL events, the NBA writes the URL as an attribute into the network event's XML metadata.

2. The NBA passes the network event and the XML metadata to a policy engine for analysis.

3. Policy engines apply Data in Motion triggers to network events captured by the NBA.
4. The Data In Motion triggers use XML [data lookup commands](#) (see page 293) to detect specific URLs in the metadata of transmitted files and other network events. If a specific URL is detected, the trigger fires.

You must configure the Data In Motion triggers to use suitable XML data Lookup commands.

Detecting URLs in Network Events

Use xmlattr lookup commands to apply policy to network events originating from specific URLs.

Syntax

To detect network events originating from specific URLs, the syntax is:

```
xmlattr WHERE apm/event/file/url <stringoperator> <URLs>
```

Where:

<stringoperator> determines that the specified URLs must be present. Example values include 'is', 'is any', 'contains', and 'contains any'. See the reference below for full details.

<URLs> specifies the URLs you want to detect.

Examples

- This example detects network events if any of the specified URLs are present:
xmlattr WHERE apm/event/file/url contains any
{ "domain.co.uk", "domain.net" }
- This example uses wildcard to detect matching URLs:
xmlattr WHERE apm/event/file/url is any
{ "http://www.domain.*", "http://login.domain.*", "http://mail.domain.*" }

More information:

[XML Attribute Lookup Examples](#) (see page 309)

[XML Attribute Lookup](#) (see page 306)

[<Stringoperator>](#) (see page 327)

Exempting URLs in Network Events

Use `xmlattr` lookup commands to exempt network events originating from specific URLs. Network events from exempted URLs are excluded from policy processing and cannot cause triggers to fire.

For example, you may want to allow traffic from the Unipraxis web site but block all other network traffic.

Syntax

To exempt network events originating from specific URLs, the syntax is:

```
xmlattr WHERE apm/event/file/url <stringoperator> <URLs>
```

Where:

`<stringoperator>` is either 'excludes' or 'excludes all'. See the reference below for full details.

`<URLs>` specifies the URLs you want to detect.

Examples

- This example exempts network events originating from `unipraxis.com`:
`xmlattr WHERE apm/event/file/url excludes "unipraxis.com"`
- This example uses wildcard to exempt multiple URLs:
`xmlattr WHERE apm/event/file/url excludes all {"unipraxis.co.uk", "unipraxis.net"}`

More information:

[XML Attribute Lookup Examples](#) (see page 309)

[XML Attribute Lookup](#) (see page 306)

[<Stringoperator>](#) (see page 327)

Chapter 19: Scanning Files and Other Items

This section summarizes how CA DataMinder can scan and apply policy to files and other items.

Note: For full details about the File Scanning Agent (FSA), see the *Stored Data Integration Guide*.

This section contains the following topics:

[How Does CA DataMinder Protect Files on the Local Hard Disk?](#) (see page 237)

[How Does the FSA Scan Stored Data?](#) (see page 239)

[Applying Policy to Scanned Items](#) (see page 241)

How Does CA DataMinder Protect Files on the Local Hard Disk?

The CFSA can run scheduled scans of the local hard disk and apply Data At Rest triggers to targeted files. The process is summarized below and in the following [flow chart](#) (see page 238).

1. CFSA applies machine policy.

Settings in machine policy determine when and how often the CFSA runs a local file scan.

Other machine policy settings identify the files and folders that you want to scan. For example, you can specify local files or folders that you want to explicitly include or exclude from the scan. You can also choose to only scan files modified since the previous scan.

2. CFSA applies user policy Data At Rest triggers.

When the scan runs, CFSA applies Data At Rest triggers in the user policy.

These triggers analyze the scanned files and apply appropriate control actions. For example, they can categorize files based on their text content. They can also add smart tags to scanned items. The smart tags are either saved with the event metadata in the CMS database or, for Microsoft Office documents, you can apply smart tags to the original document.

Finally, you can configure control actions to delete, replace, or move unauthorized files, or copy scanned files to another location for further investigation.

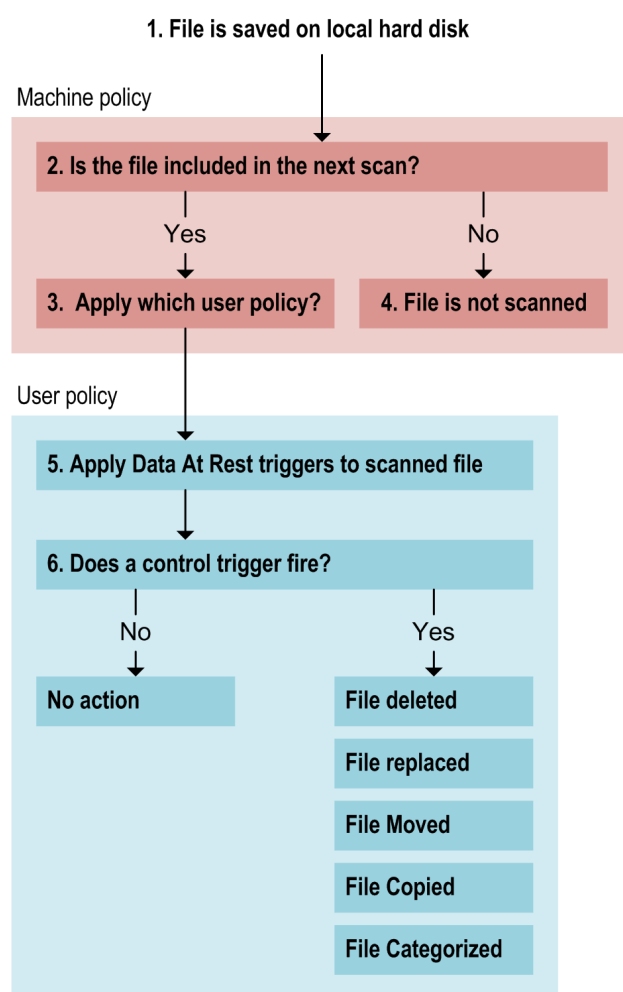
More information:

[CFSA Flow Chart: Scanned Files on Local Hard Disk](#) (see page 238)

CFSA Flow Chart: Scanned Files on Local Hard Disk

In the diagram below, a user saves a file to the local hard disk (1). When the next scheduled file scan runs, the CFSA checks machine policy to determine which files and folders to include (2) and which user policy to apply (3). Files implicitly or explicitly excluded are not scanned (4).

When the scan runs, CFSA applies Data At Rest triggers to the scanned files (5). If a control trigger fires, the CFSA applies an action to the scanned file (6). For example, they can categorize files based on their text content, and delete, replace or move unauthorized files.



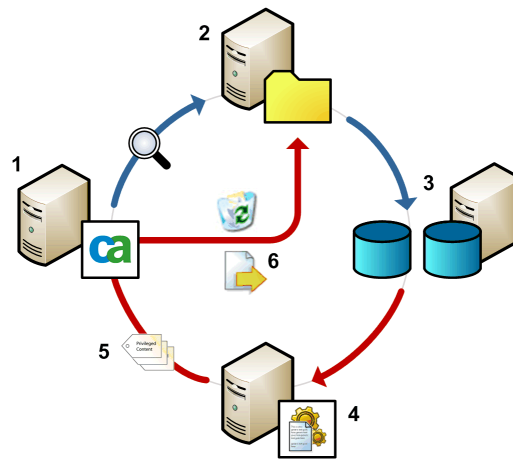
How Does the FSA Scan Stored Data?

The File Scanning Agent (FSA) integrates CA DataMinder with the stored data used by your organization. It is designed to scan, analyze and apply appropriate policy controls to:

- Files saved in local or remote file systems
- Items stored in Exchange Public Folders
- Items hosted on Microsoft SharePoint sites
- Text entries and documents stored in SQL Server or Oracle databases.

The FSA must be deployed in conjunction with CA DataMinder policy engines and a policy engine hub. It uses Data At Rest triggers to analyze and apply policy to scanned items. It only extracts text content if it is required for policy processing, making the scans highly efficient.

When a scanning job runs, an event is generated for each scanned item that causes a Data At Rest trigger to fire. All file events captured by the FSA can be viewed alongside existing e-mail, Web and IM events using the iConsole or Data Management console.



FSA: scanning procedure for files

The FSA (1) scans target folders (2) and checks files against records in the Scanned File database and, optionally, a NIST database (3). New or changed files are passed to a policy engine (4) for processing. Data At Rest triggers analyze the files and, if required, apply smart tags (5). When processing is complete, the policy engine calls back to the FSA with the processing results. Finally, the FSA then implements any applicable control actions, such as deleting specific files or copying them to a new location (6).

Which User Policy Gets Applied?

When you create a scanning job using the FSA Job Definition wizard, you must specify the policy participant. This is the CA DataMinder user account whose policy you want to apply to all scanned items.

For each scanning job, you can choose to apply the Default Policy for Files (defined in policy engines' machine policy) or you can apply a specific user's policy; to do this, you specify the user's email address. See the wizard's online help for details.

Note: You also specify the event participants when you create a scanning job. These are the users that you want to associated with the scanned items.

Applying Policy to Scanned Items

To apply policy to scanned items, you must edit the local machine policy and the user policy.

Note: Details about key policy settings are provided in the following topics.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. (Applies to CFSA local scans only) Edit the machine policy. For example:
 - a. Expand the Machine Administration branch.
 - b. Right-click the CMS and click Edit Common Client Policy.
3. (Applies to CFSA local scans only) Browse to the following folders:

Data At Rest Protection folder

Find this folder in the Client File System Agent folder.

Edit the Included Files and Excluded Files settings.

Policy Engine folder

(Optional) For performance reasons, you may need to amend settings in this folder. Only edit these settings if instructed to do so by CA technical staff.

4. Save the machine policy changes.
5. Edit the user policy.
 - a. Expand the User Administration branch.
 - b. Right-click a user or group and click Edit Policy.
6. Edit the **Data At Rest** triggers.

CA DataMinder uses Data At Rest triggers to analyze scanned items. These triggers can detect specific file names, analyze the text content, add smart tags, and (by using XML Attribute lookup commands) identify file attributes such as size, date last modified, and the document author.
7. Edit the **Data At Rest** control actions.

Data At Rest control actions can delete scanned files, or copy or move them to an alternative location.
8. Save the user policy changes.

More information:

[Configure the Local Machine Policy](#) (see page 242)

[Configure the User Policy](#) (see page 243)

Configure the Local Machine Policy

To configure the CFSA, edit settings in the Client File System Agent folder of the machine policy on each client machine. We recommend that you edit the Common Client Policy. You may also need to adjust settings in the Policy Engine folder.

The key policy settings are described in the following sections.

Policy Engine Folder

For performance reasons, you may need to amend these settings in the Policy Engines folder. You must only edit these settings if instructed to do so by CA technical staff:

Maximum Number of Concurrent Operations

Defines the maximum number of files that can be processed simultaneously by a policy engine.

Deadlock Detection Timeout (seconds)

Specifies how long a worker thread must be inactive while processing an event before the policy engine considers the thread to have stalled.

Data At Rest Protection Folder

Settings in this folder control how often the CFSA runs scheduled scans of the local hard disk. They also determine which drives, folders and files are scanned, and which user policy is applied to scanned files. This folder also includes the File System Scan Configuration subfolder.

Included Folders; Excluded Folders

These settings determine which folders to scan. By default, the CFSA scans all local folders except the \Windows and \Program Files folders, but you can change these. For example, you can specify the main folders you want to scan the Included list, but then use the Excluded list to omit specific subfolders.

By default the Excluded Folders setting uses %SystemRoot% and %ProgramFiles% variables to exclude the \Windows and \Program Files folders.

Included Files; Excluded Files

These settings determine which files to scan within the included folders. By default, the Included setting lists all the common document types such as '*.doc' and '*.ppt'. No files are excluded by default, but if required you can use the Excluded list to omit specific file types such as .mp3 or .log files.

Note: The Excluded list takes precedence if there is a conflict. For example, you can include all spreadsheets (*.xls) but exclude specific files such as 'Holiday_Form.xls'.

Default Policy for Data At Rest

This setting determines which user policy gets applied to scanned files. It defaults to 'DefaultClientFileUser'. A CA DataMinder user account with this name is created automatically when you install a CMS. This account is created specifically to apply policy to scanned files across all workstations. Or you can specify a different CA DataMinder user account (enter the user name, not the full name).

Enable File System Scan

Set this to True to set up regular scans of all included files on the local machine. If you do enable full scans, settings in the File System Scan Configuration folder allow you to set the scan frequency.

Configure the User Policy

You must edit your user policies to complete the CFSA and FSA configuration. Edit the Data At Rest triggers and control actions to protect your stored data, including files saved on the local hard disk.

Key policy settings are described in the following sections.

Data At Rest Triggers

Data At Rest triggers include general settings that let you specify which types of document you want the CFSA or FSA to scan. For example, you can edit the triggers to detect specific file formats (such as Microsoft Word documents) and analyze a file's text content. This section focuses on the key Data At Rest settings.

Which File Sources?

In each Data At Rest trigger, this setting instructs the trigger to process files or documents captured or scanned by any of the following:

- Client File System Agent
- File Scanning Agent
- File Importer
- External Agent API for File

Verify that the Client File System Agent check box or File Scanning Agent check box is selected! This enables the trigger to analyze items scanned by the CFSA or FSA respectively.

Top Level File Lists

All Data At Rest triggers include Top Level File Lists. Use these lists to detect normal files or zip files. You edit these lists to identify the names of files that you want to apply policy to when a scan runs. For example, you can specify:

- * to analyze all files
- *.docx to analyze all .docx files
- A list of specific .zip files to analyze.

For each trigger, you can choose whether to use an Included, Excluded, or Ignored file list.

Individual/Embedded File List

If required, Data At Rest triggers can look for files contained within a zip file or embedded in a master file. To do this, edit the Individual/Embedded File Lists. For each trigger, you can choose to use an Included or Excluded file list.

Using these lists in conjunction with the Top Level File Lists, you can feasibly search all .zip files for a specific file. For example, set Included Top Level Names to *.zip and Included Individual/Embedded File Names to *.doc to search for all .doc files contained within .zip files.

Copy File to Location

Data At Rest control actions also support 'copy' actions, permitting you to [copy scanned files to an alternative location](#) (see page 246). When used in combination with a 'delete' actions (see below), a copy action effectively becomes a 'move file' action.

Intervention

In each Data At Rest control action, the Intervention setting determines how CA DataMinder handles scanned files. The available options allow you to categorize or delete scanned files. If necessary, you can specify DoD deletions; these ensure that deleted files cannot be recovered (see below). You can also replace deleted files with an explanatory stub file to alleviate any user concerns or categorize the resulting file event.

DoD deletion is forensic deletion, so called because the storage media are purged to guarantee that a file cannot be recovered and used to obtain evidence in legal discovery. 'DoD' is a reference to Department of Defense approved methods for purging storage media.

Notes

- DoD deletions are not supported for scanned items in Exchange Public Folders or SharePoint sites, or for scanned database records.
- No Data At Rest control actions can be applied to scanned database records or generic items on SharePoint sites (such as Announcements and Discussion Boards). However, if SharePoint generic items have file or document attachments, the FSA *can* apply control actions to those attachments.

Apply Smart Tags to Scanned Items

CA DataMinder can apply smart tags to events generated by the FSA (that is, 'scan events' stored on the CMS). In the case of scanned Microsoft Office documents, it can also apply smart tags to the original document. For further details, see the Administration console online help; search for 'smart tags'.

Apply Smart tags to CA DataMinder Events Generated by the FSA

You can configure Data At Rest triggers to add smart tags to events generated by the FSA. For example, you can use smart tags to classify scanned files for data classification purposes. When the trigger activates, each smart tag is saved with the event metadata in the CMS database.

Apply Smart Tags to Original Microsoft Office Documents

You can also configure Data At Rest control actions, to apply smart tags to scanned Microsoft Office documents. In fact, you can apply smart tags either to the original document, or to a copy of the scanned document. Each smart tag is then saved as a new property of the scanned document or, if applying smart tags to scanned items in Exchange Public Folders, each smart tag is added as a MAPI property. For details, see the Administration console online help; search for: 'smart tags: file events'.

Note: You cannot apply smart tags to original items when scanning SharePoint sites or when scanning database records.

Copying Scanned Files

In addition to deleting or replacing files, you can also configure Data At Rest control actions to save a copy of the file in another location for further investigation. This includes Microsoft Exchange Public Folders and Microsoft SharePoint sites.

Each Data At Rest control action contains the following settings:

Copy File To Location

This setting specifies the target folder for copied files. It can be any valid UNC or local file system path. If set to a relative path, that path is combined with the original scan location (set in the job definition file) to form the actual copy location.

For example, if this setting is '..\output' and the original scan location is C:\root_folder\input, then files will be copied to C:\root_folder\output.

This setting also works in combination with the Copy Location Mode setting (see below) to create the final copy path.

Important! You must specify a path outside of the scan location defined in the job file, otherwise the copied files will get scanned again! In the associated topic, see example 5.

For this reason, we recommend a target location that begins '..\'', such as ..\Review.

Copy Location Mode

This setting modifies the Copy File To Location folder. Set it to Absolute or Relative.

In Absolute mode, files are copied directly to the Copy File To Location folder, not to subfolders. In Relative mode, files are copied to a subfolder below the Copy File To Location folder; the subfolder matches the folder structure of the file's original location.

Based on the example above, if the scan finds a file in C:\root_folder\input\ScanFolder1, and Copy Location Mode is set to:

- Absolute, the file is copied to C:\root_folder\output
- Relative, the file is copied to C:\root_folder\output\ScanFolder1 (the subfolder path is preserved)

Note: If a file with the same name already exists in the given location, CA DataMinder uses the Copy Conflict Resolution setting (see below) to determine what action to take.

Copy Conflict Resolution

Specify what action you want to take if a file with the same name already exists in the target location. Set this to:

- Discard to discard the copied file and retain the existing file.
- Overwrite to overwrite the file already in the target folder.
- Create Copy rename the copied file (but adding a numeric suffix).

More information:

[Examples of Copied Files](#) (see page 247)

Examples of Copied Files

In the examples below, the FSA or the CFSA scans the C:\MyDocs\Projects folder. This contains the file Q1sales.mpp that you want to copy elsewhere. For these examples:

FSA

The scanning job definition is set up as follows:

```
<location path="C:\MyDocs"/>
<folders subfolders="yes">
<include>Projects</include>
</folders>
```

CFSA

The Data In Use Protection folder in the local machine policy is set up to identify C:\MyDocs\Projects* as the folder you want to scan.

To copy MyProject.mpp to a new location after it has been scanned, you need to edit the relevant settings in the Data At Rest control action as follows:

Example 1: Copy File to Location is set to '..\Review'

This is the method we recommend. Again, the target location is outside the scan location defined by the <location> tag in scanning job file.

- If Copy Location Mode is set to Relative, the file gets copied to:
C:\Review\Projects\Q1sales.mpp
- If Copy Location Mode is set to Absolute, the file gets copied to:
C:\Review\Q1sales.mpp

Example 2: Copy File to Location is set to 'C:\Evaluate'

The target location is C:\Evaluate, a subfolder outside the scan location defined by the <location> tag in the scanning job file.

- If Copy Location Mode is set to Relative, the file gets copied to:
C:\Evaluate\Projects\Q1sales.mpp
- If Copy Location Mode is set to Absolute, the file gets copied to:
C:\Evaluate\Q1sales.mpp

Example 2: Copy File to Location is set to 'Review'

Important! Avoid this situation!

Here, the target location is interpreted as a subfolder below the original scan location and so the file gets scanned again!

- If Copy Location Mode is set to Relative, the file gets copied to:
C:\MyDocs\Review\Projects\Q1sales.mpp

More information:

[Copying Scanned Files](#) (see page 246)

Chapter 20: Categorizing Events

This section contains the following topics:

[Overview](#) (see page 249)

[Why Categorize Events?](#) (see page 251)

[Categorization Methods](#) (see page 251)

[How Does Categorization Work?](#) (see page 253)

[Guidelines for Categorization Control Triggers and Actions](#) (see page 257)

[Set Up New Categorization Triggers](#) (see page 261)

[Add Categorization to Existing Triggers](#) (see page 263)

[Syntax for Specifying Categories](#) (see page 265)

[Smart Tag Category Variables](#) (see page 269)

[Policy Classes](#) (see page 272)

[Trigger Severity](#) (see page 274)

Overview

CA DataMinder provides the following event categorization capabilities:

Email and file categorization

CA DataMinder can optionally assign an email or file to one or more categories. The categorization process can be fully automated, assisted, or manual.

Individual categories are defined in email, Data At Rest or Data In Motion triggers and 'categorize' options are available in policy control actions. When an email or file causes triggers to fire, the resulting control action causes CA DataMinder to analyze all categories specified in these triggers.

CA DataMinder then automatically assigns the email or file to the most appropriate category, or it displays the possible categories in a Categorize dialog.

Note: The Categorize dialog is only shown for emails or files detected by CA DataMinder endpoint agents. The dialog allows the user to choose the most appropriate categories. You can configure the dialog to list all the possible categories, or only the most likely ones.

Trigger severity

CA DataMinder assigns policy triggers to severity bands based on their severity scores. By default, the severity bands are Low, Medium, or High. For example, you may want to assign a high severity score to a trigger that detects serious violations of corporate rules. When the trigger activates, the severity score is saved with the resulting event. You can then search for events by severity in the iConsole or Data Management console.

Policy classes

You can associate individual triggers with a particular policy for a solution class. This information gets stored with the event metadata when the trigger activates. For example, if you associate the Sales Information policy with a trigger, you can run an iConsole search for events associated with this policy.

Smart Tagging

This feature enables CA DataMinder to categorize, or tag, an event captured when a specific trigger activates. Specifically, you configure a trigger to capture or detect all emails with a particular theme and to tag them accordingly. For example, you can tag emails as Personal Communication, Employment Solicitation, or Privileged Content. Smart tags are saved with the event metadata in the CMS database and can be viewed later in the iConsole by reviewers.

Document classifications

These enable CA DataMinder to detect specific types of document (emails, imported files, attachments, and web pages). For example, you can configure classifications to detect sales proposals, contract agreements, or airline web sites. Document classifications are configured in the user policy.

More information:

[Set Up New Categorization Triggers](#) (see page 261)

[Smart Tagging](#) (see page 275)

[Trigger Severity](#) (see page 274)

[Document Classifications](#) (see page 283)

[Policy Classes](#) (see page 272)

Why Categorize Events?

CA DataMinder enables you to quickly roll out a highly accurate event categorization strategy across your organization. Categorization allows you to structure your captured emails, files, and attachments. Instead of treating electronic communication as a near-uniform commodity, categorization allows:

Selective archiving

Irrelevant communications such as out-of-office notifications and email newsletters can be categorized accordingly and excluded from archiving, reducing storage requirements and increasing search performance.

Optimized storage

Precise categorization by, for example, purpose (business or personal) or regulatory implication, can allow archives to assign much more precise retention dates, eliminating the risk that a message is prematurely moved to offsite storage or even deleted.

Faster, more accurate event retrieval

With accurate categorization, the task of monitoring communications is transformed from a lottery based on random review to a process with pinpoint targeting. Reviewers can rapidly filter event searches to focus on events that truly merit individual attention.

Categorization Methods

CA DataMinder will either select the most appropriate category automatically or, for emails, allow the user to select a category, depending on the categorization method:

Fully automated categorization

CA DataMinder automatically assigns an email or file to a single category or, if applicable, to multiple categories.

- **Emails:** You can set up fully automated categorization for emails detected by both server agents and client agents, or imported as part of an Import Policy job.
- **Files:** Fully automated categorization is available for files detected by the FSA, NBA, Client File System Agent, Client Print System Agent, or imported as part of an Import Policy job.

Assisted categorization

Available only for emails, files or documents detected by a client agent.

A Categorize dialog permits the sender of an email, or a user attempting to print a document or save a file to a USB device, to choose from a short list of categories deemed most plausible by CA DataMinder, or to confirm a category automatically selected by CA DataMinder.

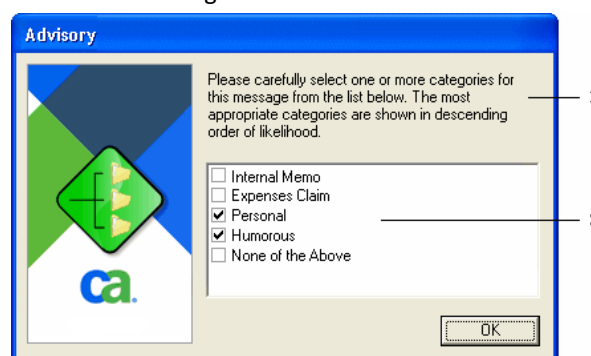
You can configure the Categorize dialog to allow the user to choose multiple categories ('multi-select') or force them to choose a single category ('single-select').

Manual categorization

Available only for emails, files or documents detected by a client agent.

The email sender, or the user attempting to print a document or save a file to a USB device, is permitted to choose from the full range of possible categories listed in a Categorize dialog.

As for assisted categorization, you can configure the Categorize dialog for multi-select or single-select.



Example Categorize Dialog

1 Configurable explanatory message. 2 Available categories.

All categorization methods can be operational at the same time within a single user policy. That is, different triggers and control actions can specify different categorization methods, and the actual method used depends on which triggers activate.

How Does Categorization Work?

When an email or file activates a trigger (or triggers), there may be multiple categories associated with these triggers. How does CA DataMinder ensure that the event is correctly categorized?

CA DataMinder either selects the most appropriate category automatically, or (for emails) allows the user to manually select a category. For emails, the actual method used, automatic or manual categorization, depends on two factors:

Client versus server agent

The first critical determinant is how the email, file or document was captured:

Client Agent Captures

For emails captured by an Outlook or Notes client agent, and files or documents captured by the Client Print System Agent or the Client File System Agent, then CA DataMinder can display the Categorize dialog and allow the user to manually choose the most appropriate categories.

Other Captures

For emails captured by an Exchange or Domino server agent or the NBA, and files captured by the FSA or NBA, or imported as part of an Import Policy job, CA DataMinder must either categorize the file or email automatically or assign no category. It cannot allow the user or sender to manually choose the category.

Category score

The second critical determinant is the category score. Each category specified in a trigger must have a category score (set by the policy administrator). CA DataMinder uses these scores to choose the most appropriate categories.

Category Scores

Each category specified in a trigger must have a category score (set by the policy administrator). There are no upper or lower limits, but typical scores range from zero to 100. The category score is an indication of confidence; the higher the score, the greater the confidence that an email fits the associated category.

CA DataMinder uses these scores when assigning categories automatically or when assisting a user to manually choose a category (or categories). The scores also determine the order in which categories are listed in the Categorize dialog.

Briefly, if you set a category score to:

100 or higher

This indicates certainty. Such scores indicate to CA DataMinder that an email or file definitely fits the associated category. Such categories are always stored with the associated event in the CMS database.

50 to 99

This indicates 'likeliness'. Such scores indicate to CA DataMinder that an email or file is likely to fit the associated category. If the highest scoring category is between 50-99:

- For emails or files detected by an endpoint agent, this category plus any others scoring 50-99 are always listed in the Categorize dialog. (Categories scoring less than 50 are not shown in the dialog; CA DataMinder assumes the file or e-mail is less likely to match these low scoring categories.)
- For emails or files detected by any other method, this category is automatically stored with the event in the CMS database.

Less than 50

This indicates some uncertainty (or possibility). If the highest scoring category is less than 50:

- For emails or files captured by a client agent, all categories are listed in the Categorize dialog. This is because, with all categories scoring less than 50, CA DataMinder cannot confidently determine the most likely categories.
- For emails or files captured by any other method, all categories are discarded. The event is saved on the CMS without an associated category because CA DataMinder cannot confidently determine what the category should be.

We recommend you include an 'None of the Above' fallback category if all your categories score less than 50.

How Do Category Scores Affect the Categorization Method?

This topic summarizes how different category scores affect the categorization method.

Fully automated categorization

For emails or files imported in an Import Policy job or detected by a server agent, FSA or NBA, CA DataMinder automatically chooses the highest scoring category, but only if the highest scoring category is 50 or above. If multiple categories score 100 or above, each of them is stored with the event.

For emails or files detected by a client agent, categorization is automatic and the Categorize dialog is not shown if:

- Any category scores 100 or above. CA DataMinder simply chooses the highest scoring category(ies).
- A single category is specified, scoring between 50 and 99.

Assisted categorization

Available only for emails, files or documents detected by a client agent.

- CA DataMinder automatically lists all categories scoring between 50 and 99 in the Categorize dialog and omits from the dialog any categories scoring less than 50. This is because CA DataMinder infers that the higher scoring categories are the more likely and restricts the user's choice accordingly.
- In all cases, categories are listed in descending order (of score) in the Categorize dialog to assist the user. That is, the most likely categories are listed first and the top scoring category is pre-selected.

Category	Score	Listed in Categorize dialog?
ISDA Confirmation	90	Yes; Preselected
OTC Contract	80	Yes
Internal Memo	40	No
Expenses Claim	20	No
Personal	20	No
Humorous	20	No
None of the Above	0	No

Manual categorization

Available only for emails, files or documents detected by a client agent.

If no category scores over 50 (that is, all are low scoring), all are listed in the Categorize dialog. For example, when specifying categories in your policy triggers, you may deliberately set very low category scores if you want to force users to choose a category manually.

Note: We recommend you include a 'None of the Above' fallback category if all your categories score less than 50. Setting the category score to zero for the 'None of the Above' category ensures that it is always listed last in the Categorize dialog.

Category	Score	Listed in Categorize dialog?
Internal Memo	40	Yes
Expenses Claim	20	Yes
Invoice	20	Yes
Personal	20	Yes
None of the Above	0	Yes

Category Score Summary

This table summarizes how the CA DataMinder client and server agents handle different category scores.

For example, if an Outlook client agent detects an email and the resulting triggers specify a single category with a score between 50 and 99, that category is automatically stored with the event on the CMS.

Conversely, if the same triggers specify multiple categories, all categories scoring over 50 are listed in the Categorize dialog ('assisted categorization') and the user must manually choose the most appropriate category.

Highest score	How many categories?	Emails or files detected by:	Emails or files detected by:
		Outlook or Notes client agent CPSA or CFSA	Exchange or Domino server agent, FSA, NBA, or Import Policy
0-49	1 only	Manual categorization: The Categorize dialog is shown and the user must manually choose the only available category.	No categorization: The category is not stored.

		Note: We strongly recommend that you prevent this situation arising by including a 'None of the Above' category.	
	2 or more	Manual categorization: The Categorize dialog is shown and the user manually chooses the category. Note: These low-scoring categories are not shown in the dialog if any other category scores 50 or higher.	No categorization: No categories are stored.
50-99	1 only	Automated categorization: The Categorize dialog is not shown and the category is stored automatically.	Automated categorization: The category is stored automatically.
	2 or more	Assisted categorization: If multiple categories assigned, the dialog is shown and the user manually chooses the category. Any category scoring less than 50 is omitted from the Categorize dialog.	Automated categorization: The highest scoring category or categories are stored automatically.
100+	1 only	Automated categorization: The Categorize dialog is not shown and the category is stored automatically.	Automated categorization: The category is stored automatically.
	2 or more	Automated categorization: The Categorize dialog is not shown. The highest scoring categories are stored automatically.	Automated categorization: The highest scoring category or categories are stored automatically.

Note: FSA = File Scanning Agent; NBA = Network Boundary Agent; CPSA = Client Print System Agent; CFSA = Client File System Agent.

Guidelines for Categorization Control Triggers and Actions

Using policy triggers, you can set up an e-mail or file categorization strategy to meet the needs of your organization. For example, can automate categorization as much as possible. Alternatively, you might prefer users to manually categorize their own e-mails. Or you can implement a combination of manual and automatic categorization.

Categorization Trigger Guidelines

Files captured by the FSA, NBA or an Import Policy job

File events captured by the FSA or NBA, or imported in an Import Policy job, can only be categorized automatically. CA DataMinder does not support manual categorization of these files. Consequently, when specifying file categories in your Data At Rest or (for NBA file events) Data In Motion control triggers, do not assign category scores lower than 50. Such low scoring categories are always discarded!

Emails and files captured by client agents

If you want to automate categorization, you can set up separate triggers for specific categories. If you then define very stringent trigger criteria, this will allow you to set a high category score (100 or higher). For example, you may have a 'customer complaint' trigger. If any email does cause this trigger to fire, you can be highly confident that it really is a customer complaint and the high category score ensures that this complaint category is stored automatically with the email.

If you want to allow manual categorization, you may prefer to define a single trigger that specifies multiple, possible categories, each with a low category score (below 50). In this case, the trigger criteria will be much less stringent in order to detect a wider range of emails. The low category scores ensure that all categories are listed in the Categorize dialog (if the email is detected by a client agent), permitting the sender to choose the most appropriate category. But see our 'None of the above' recommendation in this situation.

Note also that you can explicitly set up triggers for Outlook or Notes client agents (which permit manual categorization) and for Exchange or Domino server agents (which do not). To do this, you configure the Which E-mail Sources? trigger setting; this setting is included in all email triggers.

Similarly, you can explicitly set up Data In Motion triggers for CPSA and CFSA client agents (which permit manual categorization) and for the NBA (which does not). To do this, you configure the Which File Sources? trigger setting; this setting is included in all Data In Motion triggers.

More information:

[Guidelines for Categorization Control Triggers and Actions](#) (see page 257)

[Set Up New Categorization Triggers](#) (see page 261)

[Add Categorization to Existing Triggers](#) (see page 263)

[Do I Need a None of the Above Category?](#) (see page 259)

Do I Need a None of the Above Category?

For emails and files captured by client agents, if all your specified categories are low scoring (that is, below 50), we strongly recommend that you include a fallback category such as 'None of the Above'.

This is because, for emails detected by a client agent, CA DataMinder compels the user to choose from a list of available categories. By providing a fallback category, you allow the user to indicate the disparate nature of their file or email if none of the other categories are appropriate.

If you set up a 'None of the Above' category, note the changes to the usual syntax when specifying the category in the Message to Users trigger setting:

- Always set the category score to zero. This ensures that the 'None of the Above' category is always at the bottom of the category list in the Categorize dialog, below the other categories!
- You do not need to add a smart tag. This is because, with no definite category, there is no point storing the category information on the CMS so there is no need for a category smart tag.

Which Control Action Number?

Data At Rest control actions

For Data At Rest control actions, the control action number is not important. The categorize action, if specified, is always performed even if other control actions delete or replace the file.

Email and Data In Motion control actions

Although we recommend using the lowest possible control action number as your categorize action (because of control action precedence), we recognize this is not practical if you already use a large number of triggers and control actions.

Instead, we recommend you use the lowest available control action. For example, if Control Actions 1 to 6 are already in use, designate Control Action 7 as your categorize action. This means, for example, as long as the email is actually sent, it is categorized. If the email is not sent (because it is blocked or the sender heeds a warning), then it is not categorized; that is, the resulting event is stored on the CMS without category details. Similarly, if CA DataMinder blocks an attempt to print a document, the document is not categorized.

There are two further recommendations.

- If you use both multi-select and single-select categorize actions, the multi-select categorize action must have a lower number than the single-select action.
- You must ensure that your categorize action has a lower control action than your quarantine action. This ensures that quarantined emails are categorized before they are quarantined (emails are immune from further control actions once they enter quarantine). It is for this reason that we recommend that you configure the highest control action as your quarantine control action.

If Both Multi- and Single-Select Email Categorization Actions are Invoked

If required, you can have two categorize actions operational at the same time, one to make the Categorize dialog multi-select and the other make it single-select, the resulting Categorize dialog will always be multi-select. That is, the multi-select specification overrides the single-select regardless of the respective control action numbers.

However, the explanatory message in the Categorize dialog always derives from the control action with the lowest number (more accurately, the message is provided by the trigger that invokes the control action with the lowest number). This means that the multi-select categorize action must have a lower number than the single-select action. This ensures that the explanatory message is appropriate for a multi-select Categorize dialog (that is, it indicates that the user can choose one or more categories).

Example: Control Action 1 specifies multi-select categorization; Control Action 2 specifies single-select categorization. In the Categorize dialog, the explanatory message and multi-select list both derive from Control Action 1, but the list of categories jointly derives from both Control Action 1 and Control Action 2.

Set Up New Categorization Triggers

CA DataMinder event categorization is policy-based. This ensures that emails or files are successfully categorized, regardless of how they were captured or imported.

1. Configure a categorize control action. Your categorization triggers reference this control action in step 5. Specifically, you must specify a Categorize option for the Intervention setting. For email control actions and Data In Motion control actions, there are two Categorize options:

Categorize: Single category only

This displays a single-select Categorize dialog. The user can only select a single category for their email or file.

Categorize: Multiple categories allowed

This displays a multi-select Categorize dialog, permitting the user to select multiple categories.

Note: Because of control action precedence, we recommend that you designate the lowest possible control action number as your categorize action. For example, if you designate Control Action 1 as your categorize action.

2. Set up your categorization trigger(s). These can be any email or file control triggers. Set up the triggers to detect the emails or files you want to categorize.

How you set up the triggers depends on various factors. For example, if you are using Outlook or Notes client agents to detect emails and you want to permit users to manually categorize their emails, you can set up a single trigger that specifies multiple possible categories, each with a low category score.

3. Configure the Smart Tags trigger setting to save the final email or file category or categories—whether selected automatically by CA DataMinder or chosen by the user—as smart tags.

Important! You must add a smart tag to store the email category, otherwise the category details will not be saved on the CMS.

When you add a new smart tag, you must set its name (or value) to include a categorization variable such as %category% (this variable is populated with the category 'label' specified by the <smart tag> parameter in the Message To Users setting—see step 4). Note also:

- If you have multiple triggers that specify categories, you must configure the smart tags identically in each trigger.
- To make the smart tags readily identifiable in the iConsole, we recommend that you prefix the variables with text labels. For example:

Category: %category%

- Smart tags are case-sensitive.

4. Specify the associated category or categories. To do this, you edit the Message To Users trigger setting. Use the [correct syntax!](#) (see page 265)

Briefly, the message must include the following elements:

<message text>

Specifies the explanatory message shown in the Categorize dialog or (for files detected by the FSA) replacement stub files.

<category>

Specifies a category name that is listed in the Categorize dialog.

<score>

Is the category score.

<smart tag>

Specifies a category 'label' that gets converted to a category smart tag.

As with smart tags in Step 3, if you have multiple triggers that specify the same category, you must specify the category name and label identically in each trigger. This prevents variations in spelling or capitalization being stored as separate category smart tags for the same event.

5. Point each categorization trigger at the same control action.

Specifically, set the Control Action trigger setting to point to the categorize control action you specified in Step 1.

More information:

[Add Categorization to Existing Triggers](#) (see page 263)

[Syntax for Specifying Categories](#) (see page 265)

[Example Category Definitions](#) (see page 268)

Add Categorization to Existing Triggers

You can incorporate categorization into any of your existing email, Data At Rest, or Data In Motion control triggers. CA DataMinder event categorization has been designed to integrate with your existing user policies with minimum disruption.

For example, if you already have a warning trigger that activates when a user sends an email to an unauthorized recipient, you can include an appropriate category, or a range of possible categories, in the trigger.

1. Set up a new categorize action. But see the recommendations about the control action number.

The sole purpose of this categorize control action is to ensure that category smart tags are saved with the event on the CMS if an existing trigger fires. Without this new control action, adding categorization to your existing triggers will not work.

In your chosen control action:

- a. Set the Intervention setting:
 - For Data At Rest control actions, choose 'Categorize'.
 - For E-mail or Data In Motion control actions, choose 'Categorize: single category only' or 'Categorize: multiple categories allowed'.
 - b. Disable email and file capturing in the new control action. This ensures that emails and files are only captured if an existing trigger fires. Set the following settings to False:
 - Capture Authorized Activity?
 - Capture Prohibited Activity?
2. Modify your existing triggers to support categorization.

For each applicable trigger, edit the Message To Users setting so that its existing message is retained (for example, a warning that the current email may be non-compliant, or a notification that the original file has been replaced) but appended with a relevant category.

You do not need to change the existing Control Action trigger setting.

3. Add a single new email control trigger that explicitly invokes the categorize control action. Without this new trigger, categorization will not work.
 - a. Set the general trigger criteria. These must be sufficiently flexible so that the trigger always fires when your existing triggers fire. For example, you can set up a recipient-based trigger that fires when the recipient matches '*' (that is, the trigger will always fire).
 - b. Edit the Smart Tags setting to include a categorization variable such as %category%.
 - c. Skip this step if adding a Data At Rest trigger. If adding an email or Data In Motion trigger, edit the Message To Users setting. You need to add an explanatory message. You do not need to specify any categories; these are now specified in your existing triggers (step 2). In terms of syntax, you need only add the <dialog text>, but without double quotes and without a trailing = symbol.
 - d. The new trigger must point to the categorize control action that you set up in step 1. Set the Control Action setting accordingly.

Syntax for Specifying Categories

You define categories in the Message to Users trigger setting. Use the following syntax:

For Email and Data In Motion triggers

```
"<message text>"=
{
  "<category1>"="{ "<score>" , "<smart tag>" },
  "<category2>"="{ "<score>" , "<smart tag>" },
  "<category3>"="{ "<score>" , "<smart tag>" },
  And so on
}
```

For Data At Rest triggers

```
"<message text>"="{ "<score>" , "<smart tag>" }
```

Where:

<message text>

Specifies the explanatory message shown in the Categorize dialog (for email triggers) or replacement stub files (for Data At Rest triggers). You must enclose the message in double quotes.

For email control triggers, note the following:

- To ensure consistency in the message shown to users, we strongly recommend that you use an identical message for all triggers that invoke a single-select Categorize dialog, and a separate, identical message for all triggers that invoke a multi-select dialog.
- For new triggers, the explanatory message must clearly tell the user what action is required. This is particularly important in single-select Categorize dialogs, where there are no check boxes to indicate category selectability.

<category1>

Is only required in email triggers. It specifies a category name. This name is listed in the Categorize dialog.

- If you include the same category in multiple triggers, you must use identical spelling and capitalization, otherwise CA DataMinder will treat the variants as separate categories!
- If the category name includes double quotes (for example, "Humorous"), you must prefix the quotes with backslashes to ensure they are interpreted correctly:

```
{"\"Humorous\""}="{ \"20\" , \"Funny\" } }
```

<score>

Is the category score. We recommend you include a 'None of the Above' fallback category with a score of zero if all your email categories score less than 50.

<smart tag>

Specifies a category 'label' that gets converted to a category smart tag. You must set <smart tag> to a text string (for example, 'Customer Acknowledgment'. This text string is written to a category variable, which in turn is included in the smart tag definition. The resulting smart tag is saved with the event metadata in the CMS database. Note also:

- If you include the same category in multiple triggers, you must use identical spelling and capitalization for the <smart tag> text string, otherwise CA DataMinder will treat the variants as separate smart tags!
- You do not need a <smart tag> category label if defining a 'None of the Above' category. This is because, with no definite category, there is no point storing the category information on the CMS so there is no need for a category smart tag.

More information:

[Adding Categories to Existing Triggers](#) (see page 267)

[Example Category Definitions](#) (see page 268)

Adding Categories to Existing Triggers

To add categories for existing triggers, you need to amend the existing Message to Users setting. Specifically, you must append the new category(ies) to the existing message. Note that the original message must be enclosed in double quotes, followed by an = character, then appended with the category details.

Email trigger example

If the existing setting is:

```
This email refers to prospective M&A activity and may contravene  
corporate guidelines. Click Cancel to accept this warning.
```

You can change it to:

```
"This e-mail refers to prospective M&A activity and may contravene  
corporate guidelines. Click Cancel to accept this warning."=  
{  
  "<Unauthorized M&A reference>"=  
  {"80", "Acquisition_reference"}  
}
```

Data At Rest trigger example

If the existing setting is:

```
The previous version of this file contained confidential data  
and has been deleted.
```

You can change it to:

```
"The previous version of this file contained confidential data  
and has been deleted."=  
{"80", "Confidential_info"}
```

More information:

[Syntax for Specifying Categories](#) (see page 265)

[Example Category Definitions](#) (see page 268)

Example Category Definitions

Single-Select Example

This example Message to Users setting defines five possible categories, each with a category score between zero and 40, to display in a single-select Categorize dialog. Note that the 'None of the Above' category has no smart tag label.

"Please select one category for your e-mail from the list below.
Categories are listed in descending order of likelihood, and the
most likely category is highlighted."=

```
{  
  "Internal Memo"={"40", "Memo"},  
  "Expenses Claim"={"20", "Expenses"},  
  "\"Humorous\""={"20", "Funny"},  
  "Personal"={"20", "Personal_mail"},  
  "None of the Above"={"0"}  
}
```

Multi-select Example

This example Message to Users setting defines the same five categories as above to display in a multi-select Categorize dialog. This time, the explanatory message states explicitly that the user can choose multiple categories.

"Please select one or more categories for your e-mail from the list
below. Categories are listed in descending order of likelihood, and
the most likely category is pre-selected."=

```
{  
  "Internal Memo"={"40", "Memo"},  
  "Expenses Claim"={"20", "Expenses"},  
  "\"Humorous\""={"20", "Funny"},  
  "Personal"={"20", "Personal_mail"},  
  "None of the Above"={"0"}  
}
```

More information:

[Adding Categories to Existing Triggers](#) (see page 267)

[Syntax for Specifying Categories](#) (see page 265)

Smart Tag Category Variables

Note: Smart tags are not applicable to Microsoft SharePoint items.

When policy processing is complete, CA DataMinder saves the chosen category (or categories) to a specific variable. Additional variables can be used to store category scores and details of the three next highest scoring categories.

For any trigger that invokes a 'categorize' control action, you must specify these variables as smart tag names or values. This ensures that the chosen category, or even the 'near miss' categories, are stored with the event metadata as smart tags on the CMS.

Smart tags must be consistent!

Important! If you have multiple triggers that specify a categorize control action, you must configure the smart tags identically in each trigger! This prevents, for example, variations in spelling or capitalization being stored as separate smart tags for the same event. For example, CA DataMinder would store 'Reply to Customer' and 'Reply to customer' as two separate smart tags.

Category Variables

When setting up your categorization triggers, you can enter variables such as %category% and %categoryscore% as smart tag names or values.

Do I store categories as smart tag names or values?

How you assign category variables to smart tag names and values has a significant effect on how the smart tags are displayed in the iConsole Search Results screen. Note also that you cannot use the iConsole to search for events by smart tag value.

Available Variables

When policy processing is complete, CA DataMinder saves the chosen category (or categories) to one of these variables. You can specify these variables as smart tag names or values in your categorization triggers.

%category%

When the smart tags are generated, this variable is replaced by the selected category.

If an email or file was assigned to multiple categories, a separate smart tag is generated for each category.

%categoryscore%

When the smart tags are generated, this variable is replaced by the score for the selected category.

If an email or file was assigned to multiple categories, a separate smart tag is generated for each category.

%closestcategories%

The three 'near miss' categories in a comma separated list. These are the three highest scoring categories that did not 'win' and which each scored 50 or above.

When the smart tags are generated, this variable is replaced by a comma separated list of up to three near miss categories. These can be useful additional indicators about an email's or file's content.

If a smart tag value configured with an insertion variable (for example, %closestcategories%) is empty after that variable has been substituted (because there were no closest categories available), then the smart tag is not stored on the CMS.

Note: 'Near miss' categories are the three highest scoring categories that remain after the selected category is removed from the list.

%scoredclosestcategories%

As for %closestcategories%, but the category score is appended to each near miss category. The resulting smart tag takes this format:

Expenses (40), Hotels (30), Travel (30)

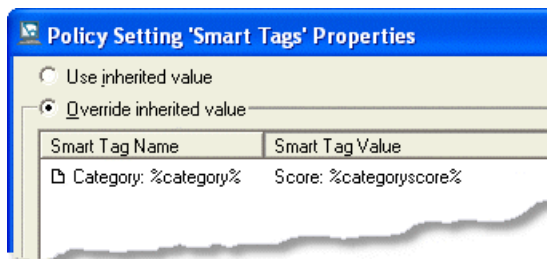
Smart Tag Guidelines for Categories and Category Scores

How you assign category variables to smart tag names and values has a significant effect on how the smart tags are displayed in the iConsole Search Results screen.

The examples below show the effect of different approaches. For optimum clarity and searchability, we recommend you use example 1.

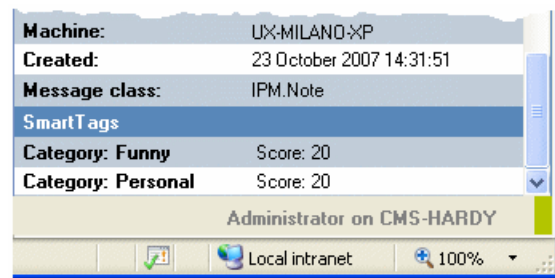
User Policy Editor, Smart Tags Properties dialog

- Smart Tag Name: Category: %category%
Smart Tag Value: Score: %categoryscore%

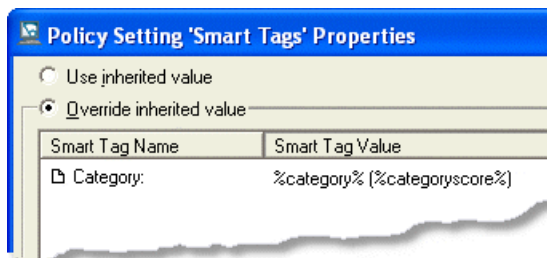


iConsole Search Results screen

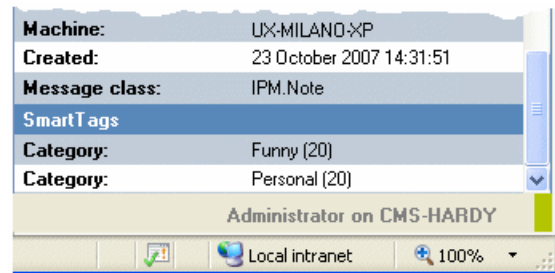
We recommend this configuration. Smart tags are readily identifiable in the iConsole. You can also search by category because individual categories are stored as smart tag names.



- Smart Tag Name: Category
Smart Tag Value: %category% (%categoryscore%)

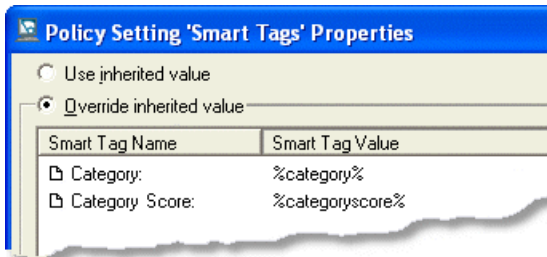


Although individual smart tags are readily identifiable in the iConsole, you cannot search for specific smart tags because this information is stored as smart tag values.



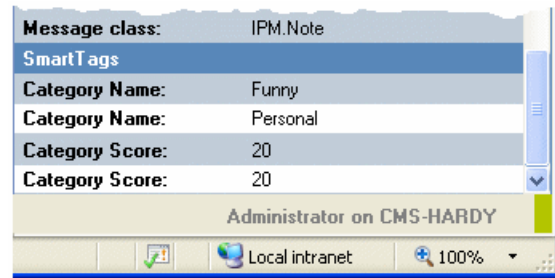
User Policy Editor, Smart Tags Properties dialog

- 3 Smart Tag Name: Category
 Smart Tag Value: %category%
 Smart Tag Name: Category Score
 Smart Tag Value: %categoryscore%



iConsole Search Results screen

Do not use this configuration. It splits an event's category and category score into two separate smart tags, making it impossible to identify an individual category's score in the iConsole.



Policy Classes

CA DataMinder contains several *policy classes* (such as Non Public Information). In turn, each policy class is implemented through various *policies* (such as Sales Information). For categorization purposes, you can associate individual triggers with a particular policy class. This information gets stored with an event's metadata when the trigger activates. All triggers support policy classes. You can then use the iConsole to search for events associated with a policy class.

Policy classes also underpin the policy-based security model. Under this model, a reviewer is only permitted to see events captured by specific classes of trigger.

Note: Find details of how CA DataMinder stores policy classes as ClassUID values in the 'Policy Classification Nodes' section under the Wgn3ClassificationNode table description in the *Database Schema and Views Reference Guide*.

Manage Policy Classes

You can define custom policies and a brief text description, for example, 'Corporate Criticism' or 'Offensive Language'. You can also organize your custom policies into classes, modify, and delete them. Default policy classes are predefined in the CMS database and you cannot edit or delete them.

Follow these steps:

1. Expand the Machine Administration branch and select the CMS.
2. Click Tools, Manage Custom Policies.

The Manage Custom Policies dialog displays existing policy classes plus the policies assigned to each policy class.

3. (Optional) Add a new policy class:
 - a. Select the top-level Custom item.
 - b. Click New Policy Class.
4. Add a new policy:
 - a. Select a policy class.
 - b. Click New Policy.
5. You can now edit user policies to associate triggers with the new policy.

More information:

[Policy Classes](#) (see page 272)

Associate Triggers with Policy Classes

When you edit a user policy in the Administration console, each trigger includes a Policy Class setting. When you edit this setting, a dialog lists all the available policy classes, including your new custom classes.

Follow these steps:

1. In the User Policy Editor, select the trigger you want to configure.
2. Expand the trigger folder, then right-click the Policy class setting, and click Properties.
3. In the Policy Class Properties dialog, expand the tree of predefined and custom classes to select a policy class for the current trigger.
4. Save the policy changes.

The trigger is associated with the policy class.

Trigger Severity

CA DataMinder can group policy triggers into bands based on their severity scores. By default, the severity bands are Low, Medium or High. For example, you may want to assign a high severity score to a trigger that detects serious violations of corporate rules.

CA DataMinder uses the following thresholds to assign triggers to severity bands:

- Not specified, or zero: No Severity
- Low Severity: 1-100
- Medium Severity: 101-200
- High Severity: 201 or greater

When one or more triggers activate, the highest severity score is saved with the resulting event. You can then search for events by severity in the iConsole or Data Management console.

To assign a severity score to a control trigger

1. In the User Policy Editor, select the control trigger you want to configure.
2. Expand the trigger folder, then right-click the Severity setting and choose Properties.
3. In the Severity Properties dialog, enter a severity score for this trigger. This must be a whole number and greater than 0.
4. Save the policy changes.

Chapter 21: Smart Tagging

This section contains the following topics:

[Overview](#) (see page 275)

[Set Up a Smart Tag](#) (see page 276)

[Example Trigger Usage](#) (see page 277)

[Smart Tags and File Events](#) (see page 278)

[Smart Tag Names and Values](#) (see page 279)

[Use Variables as Smart Tag Values](#) (see page 279)

[X-Headers and Smart Tags](#) (see page 280)

Overview

Note: Not applicable to Microsoft SharePoint items.

The Smart Tagging feature enables CA DataMinder to accurately categorize events at the time of capture.

The Smart Tags setting in each policy trigger defines the tag associated with that trigger. For example, you can assign to any trigger a tag such as Privileged Content or Employment Solicitation. When the trigger activates, this tag is saved with the event metadata in the CMS database.

Each smart tag has a name. As an optional level of sub-categorization, each tag can have multiple values. When defining smart tag values, you can also use variables to represent certain types of information.

More information:

[Overview](#) (see page 249)

[Smart Tagging](#) (see page 275)

Set Up a Smart Tag

First, you must define your smart tags in user policy triggers. A tag can be any category or descriptive term you choose. For example, you may want to tag emails as Discussion of Financial Records, Personal Communication, Employment Solicitation, or Privileged Content. All triggers support smart tags.

When the policy changes are complete, CA DataMinder categorizes each email (or attachment, imported file, Web page, or uploaded file) that activates the trigger with the specified smart tag.

To set up a smart tag

1. In the User Policy Editor, select the trigger you want to configure.
2. Expand the trigger folder, then right-click the Smart Tags setting and choose Properties.
3. In the Smart Tags Properties dialog, click Add and specify a Smart Tag Name and, optionally, a Smart Tag Value.
4. Save the policy changes.

More information:

[Smart Tagging](#) (see page 275)

Example Trigger Usage

For example, you can assign the same smart tag, 'Privileged content' (used to categorize emails subject to client-attorney privilege), to separate outgoing email triggers:

Recipient-based trigger

The first trigger activates when it detects an email sent to a specific attorney. For example, in the Recipient 1 trigger, you can set the Included Addresses list setting to include the various email addresses of the relevant attorneys.

Classification-based trigger

The second trigger activates when it detects an email that appears to be subject to client-attorney privilege. For example, in the Document Classifier 1 trigger, you can set the Which Document Classification? setting to a predefined 'Privileged content' document classification.

In this way, the recipient-based trigger should detect emails that are subject to client-attorney privilege but which do not match the specified 'Privileged content' classification, while the classification-based trigger should detect emails that are also subject to client-attorney privilege but which are not addressed to one of the listed attorneys.

More information:

[Smart Tagging](#) (see page 275)

Smart Tags and File Events

You can configure Data At Rest and Data In Motion capture and control triggers to apply smart tags to files using the Smart Tags setting.

Data At Rest triggers

You can configure Data At Rest triggers to apply smart tags to any targeted files and their corresponding file events. This can be useful for records management categorization purposes.

You can specify that when a Data At Rest trigger activates, certain smart tags are applied to the original scanned file and others to the copy of the scanned file. To do this, you need to add the exact smart tag names (or use the ? and * wildcards) to the Apply Which Smart Tags to Original File? and Apply Which Smart Tags to File Copy? control action settings.

Note: To create a copy of the original file, you need to configure the Copy File to Location control action setting.

Smart tags are stored in the file event's metadata on the CMS database. They can also be stored as a file system property, document property, or MAPI property, depending on the type of data being scanned. That is, if the FSA is scanning:

- **Microsoft Office documents**, then each smart tag is added as a document property, and can be viewed within the file itself.
- **Microsoft Exchange Public Folders** (for example an email), then each smart tag is stored as a MAPI property of the email itself.

Note: The FSA can read these MAPI properties in subsequent scanning jobs; you specify which MAPI properties to extract in the FSA job definition wizard.

Data In Motion triggers

If required, you can configure Data In Motion triggers to add smart tags to file events generated by the Network Boundary Agent, Client File System Agent (CFSA) and Client Print System Agent (CPSA). This can be useful to monitor potentially sensitive files being moved across a network, or sent to USB devices or printers. Smart tags are stored in the file event's metadata on the CMS database.

More information:

[Smart Tagging](#) (see page 275)

Smart Tag Names and Values

Each smart tag has a name. As an optional level of sub-categorization, each tag can also have one or more values. The value can be a key word or phrase, or it can be a variable. You can then display these values in the iConsole search results screen to provide at-a-glance contextual information for reviewers.

Example

Two triggers, Recipient 1 and Document Classifier 1, both apply the 'Privileged content' smart tag. In this example, you could set up smart tag values to indicate the reason that the trigger fired:

- For the Recipient 1 trigger, set the tag value to 'Matches attorney address'.
- For the Document Classifier 1 trigger, set the tag value to 'Matches document classification'.

Trigger	Smart tag name	Smart tag value
Recipient 1	Privileged content	Matches attorney address
Document Classifier 1	Privileged content	Matches document classification

More information:

[Smart Tagging](#) (see page 275)

Use Variables as Smart Tag Values

When defining smart tag values, you can use variables to represent certain types of information and to customize the text content based on the circumstances of the event capture. For example, if a smart tag has a value of %To%, this sets the tag value to the email addresses of the recipients.

The full range of supported variables are the same as those available for notification messages. Common variables for smart tag values are as follows:

Variable	Notes
%Address%	Displays the email address, or addresses, that caused the trigger to activate. For outgoing emails, this is the recipient address(es); for incoming emails, it is the sender address.
%From%	Displays the original sender of an email.

%Keystring% and %Keyword%	Displays the words or phrase detected by CA DataMinder and which activated the trigger.
%To%	Displays any recipients listed in the To: field of an email.

Smart tag variables for captured files

Because CA DataMinder can detect and capture files across multiple channels, certain variables are ideal for use as smart tags in order to categorize captured files.

Smart tag variables for categories

There is a special set of smart tag variables that can only be used in conjunction with 'categorization' email control actions.

More information:

[Smart Tag Category Variables](#) (see page 269)

[Variables in User Notifications for File Events](#) (see page 357)

X-Headers and Smart Tags

CA DataMinder enables you to insert x-headers into emails through the use of special smart tags.

X-headers are custom or proprietary headers in an Internet Mail. They are typically used to pass information to emailing applications for processing or as an information repository. For example, you can use x-headers to flag emails that require processing by a third-party encryption solution.

The mechanism that CA DataMinder uses to generate x-headers is based on the Smart Tags setting in email triggers. When the trigger activates, a smart tag is generated that matches the required x-header. CA DataMinder then detects this smart tag and sets an email property. This property is subsequently converted to an x-header when the email is sent as an Internet Mail.

Note: An x-header is only inserted if the email is actually sent. For example, if a trigger causes an email to be blocked, an x-header is not inserted.

To generate and insert an x-header

1. Agree the x-header name with the third party, for example:
X-UNIPRAXIS-MsgSec
2. In the User Policy Editor, configure your email triggers as required. For example, you may want to detect emails containing confidential information.
3. For each trigger you configured in step 2, edit the Smart Tags setting.
 - a. In the Smart Tags Properties dialog, click Add.
 - b. Set the smart tag name to the name you agreed in step 1. The name can be any text string but it must start with: X-
 - c. The smart tag value is optional. Any text you enter here (such as 'Encryption Request') will be appended to the x-header in the format:
X-UNIPRAXIS-MsgSec: Encryption Request
4. Save the policy changes.

X-headers and Domino servers

To ensure that x-headers specified by CA DataMinder are generated in Internet emails resulting from Lotus Notes emails, you must first make a configuration change on your Domino servers. For details, see the *Platform Deployment Guide*; search 'x-header handling, and Domino configuration'.

X-header Requirements

Be aware that any x-headers generated from CA DataMinder user policies must adhere to the following requirements:

X-header names must start with X—

x-header names must start with X— or x—. CA DataMinder specifically checks for 'x hyphen' smart tags when generating x-headers.

X-header names must be strong

This is crucial. When agreeing the x-header name with a third party, you must choose a 'strong' name. That is, choose a name that will not conflict with other x-headers. Specifically, avoid names that are generic or too short.

Notes and Domino users must also take care to choose x-header names that (when they have been stripped of the x— prefix) do not conflict with object names used internally by Domino.

An example of a strong x-header name is:

X-Unipraxis-MessageEncryptionRequest

Maximum length, x-header names and values

X-header **names** cannot be longer than 125 characters. Therefore, your smart tag name is similarly restricted. That is, the name you supply when editing the Smart Tags setting cannot be longer than 125 characters.

X-header **values** must not exceed 2,000 characters. X-header values are appended to the x-header name.

Although an x-header value is unlikely to be constrained by this limit, it may become more relevant in future CA DataMinder releases. For example, if a future release permits users to generate x-header values from tokens or variables (such as a 'distribution list' variable), this could potentially result in very long text strings.

Note: These x-header name and value limits are imposed by the technologies underlying the email systems (such as Outlook or Exchange). They are not inherent restrictions in the specification of Internet Mails.

X-headers cannot be added to encrypted or digitally signed emails

CA DataMinder Outlook endpoint agents cannot add x-headers to emails that have been encrypted or digitally signed.

Note: This limitation does not affect the Exchange server agent, though any policy triggers configured to detect email content may be unable to process encrypted emails anyway.

More information:

[X-header Limitation in Exchange 2003](#) (see page 170)

[X-Headers and Smart Tags](#) (see page 280)

X-header Limitation in Exchange 2003

Problems in Exchange 2003 cause the following x-header limitation for outgoing emails processed by a CA DataMinder Outlook endpoint agent and subsequently sent using Exchange.

Do not include periods in x-header names

If your x-header name includes a period character (such as X—Case.ID), Exchange 2003 will fail to insert the x-header into the email. In detail, although the Outlook endpoint agent successfully sets the appropriate email property, Exchange 2003 subsequently fails to convert this property to an x-header when this email is sent as an Internet Mail.

Note: This limitation has been fixed in Exchange 2007. Likewise, this limitation only applies to outgoing emails processed by the Outlook endpoint agent; it does not apply to emails processed by CA DataMinder Exchange or Domino server agents or the Notes endpoint agent.

Chapter 22: Document Classifications

This section contains the following topics:

[Overview](#) (see page 283)

[Classification Types](#) (see page 284)

[Setting Up a Document Classification](#) (see page 284)

[Classification Parameters](#) (see page 285)

[Parameter 6 Functions](#) (see page 288)

[Wildcards and Special Characters in Document Classifications](#) (see page 291)

[Document Classifier Triggers](#) (see page 292)

Overview

Document classifications enable CA DataMinder to detect specific types of document, for example, sales proposals, contract agreements, or airline Web sites.

When are document classifications used?

This feature is used by Document Classifier triggers. You can associate any classification with these triggers. When the trigger activates, CA DataMinder compares the active document (for example, this could be an e-mail or attachment, or a scanned file) against the specified classification. If it confirms the match, the trigger action is invoked.

Classification parameters

Each document classification uses parameter settings to identify document types defined by you. These parameters contain the rules that enable CA DataMinder to identify specific types of document, for example, sales proposals or contract agreements.

When classifying a document, CA DataMinder calculates a document score, based on the classification parameters. It uses this to quantify the probability that, for example, an e-mail attachment really is a sales proposal.

Classification Types

In the user policy, each document classification has a configuration setting. This broadly determines the type of document. At present, you can configure a classification to identify Generic or Travel documents.

Generic

These use parameter settings to identify generic document types defined by you. These parameters contain the rules that enable CA DataMinder to identify specific types of document, for example, sales proposals or contract agreements.

Travel Classifications

Less commonly used, these identify any travel-related documents, for example, Web sites for hotel or airline reservations, e-mail bookings and e-mail confirmations. Travel classifications do not use parameter settings.

When classifying a document, CA DataMinder calculates a document score, based on the classification parameters. It uses this to quantify the probability that, for example, an e-mail attachment really is a sales proposal.

Setting Up a Document Classification

First, you must define your classification in the user policy. This classification can be any type of document identifiable by its text content. For example, you may want to identify airline reservation Web sites or email customer complaints.

Second, you associate the classification with a Document Classifier trigger. These triggers are available in all Capture and Control folders. For example, you can use a capture trigger to capture the complaint email.

When the policy changes are complete, CA DataMinder detects each Web page, uploaded file, email or attachment that matches the document classification and reacts accordingly.

To set up a document classification in the user policy

1. Define your classification:
 - a. Go to the System Settings, Document Classifications policy folder.
 - b. Expand the Classification folder you want.
 - c. Enter a name for the classification and set the Configuration setting to 'Generic' or 'Travel'.
 - d. If setting up a generic document classification, configure Parameters 1 to 7.
2. Define your Document Classifier trigger.
3. Save the policy changes.

Setting a File Size Limit

You can specify a limit on the maximum size of files to be classified. To do this, you edit the Maximum Size of Files setting in the user policy System Settings folder.

Note: To ensure that files of any size are classified, set Maximum Size of Files to a value of zero.

Classification in Emails

Document classification works slightly differently with emails than with other targeted items (files and Web pages). In terms of classification, each part of an email is treated as a separate document, that is, the subject and body text are treated as one document and any attachments are also treated separately. The Document Classifier triggers are then applied to each 'document'.

The trigger will only fire if one whole document contains all the criteria in the trigger. If all parts of the email meet the classification then the score is based on the document that scored the highest.

Classification Parameters

The parameters for classifying documents are:

Parameter 1

This defines a list of compulsory words or phrases. All **MUST** be present for CA DataMinder to confirm a document classification. If validated, this parameter raises the document score by +1. In effect, this parameter specifies a Boolean AND condition.

Parameter 2

This defines a list of required words or phrases, one of which **MUST** be present for CA DataMinder to confirm a document classification. If validated, this parameter raises the document score by +1. In effect, this parameter specifies a Boolean OR condition.

Parameter 3

This defines a list of preferred words or phrases. These are positive-indicators. If any are present, this increases the probability that the document matches the specified classification. CA DataMinder raises the document score by +1 for each occurrence of a listed word or phrase.

Parameter 4

This defines a list of words or phrases that imply a possible non-match. These are negative-indicators. If any are present, this lowers the probability that the document matches the specified classification. CA DataMinder reduces the document score by -1 for each occurrence of a listed word or phrase.

Parameter 5

This defines a list of words or phrases that indicate a definite non-match. If any are present, the document classification fails. If none are present, CA DataMinder raises the document score by +1. In effect, this parameter specifies a Boolean NOT condition.

Parameter 6

You can include functions to modify the document score that CA DataMinder uses to confirm a document classification. For example: MinScore(n) and MaxScore(n) specify respectively the minimum and maximum scores necessary to confirm document classification.

Parameter 7

This defines a list of key words or phrases that you can use to search for events captured by a Document Classifier trigger. If a word is found in the document when the Document Classifier trigger activates, the word is saved as an attribute of the capture or control event. You can then run searches that focus exclusively on documents containing this word or phrase.

For example, if you define a document classification for sales proposals, you can add a list of products to parameter 7. If CA DataMinder detects one of these product names (say, Product X), in a captured sales proposal, the term 'Product X' is saved as an attribute of this event. This enables you to generate a report focusing on all sales proposals for Product X.

Note: For details about the extensive search text variables available when defining parameter 7, see the [Search Text Syntax](#) (see page 383) appendix.

Parameter 8

This defines a list of 'definite match' words or phrases. If any are present, CA DataMinder effectively confirms the document classification.

This parameter is useful if you need to detect specific types of Web site, typically those with limited text content. For example, a Web-based email site may contain very little text except for the term 'webmail'.

Note: In technical terms, this parameter overrides the Boolean conditions of Parameters 1, 2 and 5 and adds 100 onto the document score.

Parameters 9 and 10

These are not currently used in generic classifications.

More information:

[Example Document Classification](#) (see page 380)

Parameter 6 Functions

You can add these functions to parameter 6 to modify the document score handling:

Important! ReduceBySize(r) and Normalize(m) are alternative methods for adjusting document scores downwards. Do not include both functions together when specifying parameter 6.

MinScore(n) and MaxScore(n)

These define the minimum and maximum document scores needed for CA DataMinder to confirm a document classification. They can be used individually:

- Enter MinScore(n) where n is the value. For example, type MinScore(10) to set a minimum score of 10.
- Enter MaxScore(n) where n is the value. For example, type MaxScore(10) to set a maximum score of 10.

If you use MinScore(n) and MaxScore(n) together, you can define 'Significance' ranges for document classification scores. For example:

Classifier 1

Parameter 3: %CCN%

Parameter 6: MaxScore(10)

Significance: Low

Classifier 2

Parameter 3: %CCN%

Parameter 6: MinScore(11),MaxScore(100)

Significance: Medium

Classifier 3

Parameter 3: %CCN%

Parameter 6: MinScore(101)

Significance: High

Where:

Classifier 1 specifies that detecting less than 10 credit card numbers qualifies as low significance.

Classifier 2 specifies that detecting 11-100 credit card numbers qualifies as medium significance.

Classifier 3 specifies that detecting more than 100 credit card numbers qualifies as high significance.

ReduceBySize(r)

This function adjusts the document score downwards in order to prevent false confirmations, especially for long documents such as email attachments or uploaded files.

Enter `ReduceBySize(r)` where `r` determines the value subtracted from the document score; `r` is typically a very small value, for example, 0.3. The formula for this function is:

$$\text{NDS} = \text{ODS} - (\text{Characters} * (r/100))$$

Where:

Characters is the number of characters in the document.

NDS is New Document Score

ODS is Old Document Score

For example, if the original document score is 45, and the document size is 10,000 characters (a typical size for a four or five page document), then setting `r` to 0.3 lowers the document score to 15:

$$15 = 45 - (10,000 * 0.003)$$

Note: This function can result in fractional scores. Such scores are rounded to the nearest integer before testing against `MinScore(n)` or `MaxScore(n)`.

Normalize(m)

This also adjusts the document score downwards in order to prevent false confirmations. It is an alternative method to `ReduceBySize(n)`.

Enter `Normalize(m)` where `m` determines the multiplier used to lower the document score; typically, `m` matches the average size (in characters) of the documents you want to classify, for example, 10,000. The formula for this function is:

$$\text{NDS} = \text{ODS} * (m/\text{Characters})$$

Where:

Characters is the number of characters in the document.

NDS is New Document Score

ODS is Old Document Score

For example, if the original document score is 45, and the document size is 25,000 characters, then setting `m` to 8,500 would lower the document score to around 15:

$$15.3 = 45 * (8,500/25,000)$$

Note: This function can result in fractional scores. Such scores are rounded to the nearest integer before testing against `MinScore(n)` or `MaxScore(n)`.

NotSmallerThan(x)

This function defines a minimum document length. CA DataMinder does not attempt to classify documents with fewer than x characters (excluding white spaces and characters such as carriage returns). This is useful if you know the typical size of your target documents. For example, to ignore documents smaller than 500 characters, enter:

```
NotSmallerThan(500)
```

You can use this function in conjunction with its NotLargerThan(y) counterpart to define the permitted size range for target documents.

NotLargerThan(y)

This function defines a maximum document length. CA DataMinder does not attempt to classify documents with more than y characters (excluding white spaces and characters such as carriage returns). This is useful if you know the typical size of your target documents. For example, to ignore documents larger than 2000 characters, enter:

```
NotLargerThan(2000)
```

You can use this function in conjunction with its NotSmallerThan(x) counterpart to define the permitted size range for target documents.

Extract(1,2,3,4,8)

This function causes keystings found using the classification parameters 1, 2, 3, 4 and 8 to be extracted and saved as an attribute of the capture or control event. You can extract the keystings found using any or all of these classification parameters. For example, if you are only interested in the keystings found using parameters 1, 2 and 8, enter:

```
Extract(1,2,8)
```

Wildcards and Special Characters in Document Classifications

When defining document classification parameter values, note the following wildcards and logical operators:

Special characters

The following characters have special meaning and must be prefixed with a backslash if searching for literal occurrences.

{ } | [] % ? * \

For example, add \? to match any occurrence of '?'. See the reference below for more examples.

Wildcards

Wildcard characters * and ? are supported. For example, Unipr* would match any occurrence of Unipraxis.

Logical OR

Use the | symbol to represent a logical OR; For example, motel|hotel matches 'motel' or 'hotel'.

{ } sub-expressions

Use {} brackets to specify sub-expressions. For example, {motel|hotel} reservation matches 'motel reservation' or 'hotel reservation'.

Monetary values

Use %MONEY% to match any monetary value. For example, this matches \$25, \$25.99 or even 25.99. It detects \$, £ and € currency symbols, and these currency codes: USD, GBP and EUR.

Social Security numbers

Use %SSN% to match social security numbers. CA DataMinder uses a sophisticated recognition process to cross-check against an imported system definition file (US Social Security High Group File) listing currently available SSNs. For example, this matches 123-45-6789 if it is listed in the current system definition file.

Important! After June 2011, the method for generating US Social Security Numbers was modified. Numbers issued after this date are not guaranteed to match numbers in the High Group File. Do not use %SSN% if you want to detect social security numbers issued after this date.

More information:

[Special Characters](#) (see page 137)

Document Classifier Triggers

Each user policy contains Document Classifier triggers. These can check targeted items (Web pages, uploaded files, e-mails, imported files, or attachments) to see whether they match a particular document classification. You select the classification, and you specify which items are checked against this classification.

When CA DataMinder detects that an item matches a document classification:

- Control triggers generate a control event such as a blocking or warning.
- Capture triggers cause the item to be captured.

Document Classifier Triggers and Key Text

(Applies to email control triggers only.)

If an email matches the document classification you can block the email or display a warning based on the presence or absence of specific words or phrases. For example, you may want to block outgoing sales proposals if they do not contain your corporate disclaimer. To do this, add an extract of this disclaimer to the Excluded Search Text list. Here is a typical example:

This email may contain confidential or privileged information and is for use by the addressee only.

If CA DataMinder infers that an email is a sales proposal but does not contain the corporate disclaimer (because the above extract is missing), the email is blocked.

Chapter 23: Data Lookup

This section contains the following topics:

[Overview](#) (see page 293)

[User Attribute Lookup](#) (see page 297)

[Address Book Lookup](#) (see page 301)

[Message Attribute Lookup](#) (see page 304)

[XML Attribute Lookup](#) (see page 306)

[Command Variables](#) (see page 313)

[Complex Data Lookup Commands](#) (see page 338)

[Counting Unique Domains](#) (see page 344)

Overview

Data Lookup settings are available for all email, Data In Motion and Data At Rest capture and control triggers. They provide highly flexible extensions to these triggers. The following data lookup types are supported:

User Attribute lookup

User attributes are customized properties for CA DataMinder user accounts.

Data In Motion triggers can selectively detect (or exempt) files being copied, saved, or printed based on the account attributes of the CA DataMinder user.

Email triggers can selectively detect (or exempt) emails based on the account attributes of the CA DataMinder sender or recipients.

For example, if you created a 'Department' attribute for your organization, you can modify policy triggers to warn against emails sent to CA DataMinder users who belong to specific departments.

Address Book lookup

Email triggers can selectively detect (or exempt) internal emails based on Outlook Address Book properties of the recipients or the sender. For example, they can block emails sent to users in a particular office. Or they can exempt emails from being blocked if a manager is included in the recipients.

Message Attribute lookup

These lookups provide access to information contained in an email that is not accessible through any other trigger test. For example, they can detect whether emails are DRM-protected, digitally signed or encrypted.

They can also test the number of recipients, their email addresses and display names, and the size of the message including attachments. They can also detect emails based on their potential impact on network traffic. For example, they can block emails if the number of recipients is excessive or if the email is too big. (Message impact tests are primarily applied to outgoing emails. There is little point testing incoming emails).

XML Attribute lookup

These lookups enable policy triggers to test targeted files and emails for metadata attributes (this metadata is stored in XML format).

For example, file metadata includes details about the file creation and modified dates, the file name and path or URL, its title and author. The full range of available metadata varies according to the file type.

XML Attribute lookups are also used to detect x-headers in emails. X-headers are custom or proprietary headers in an Internet Mail. They are typically used to pass information to emailing applications for processing or as an information repository.

More information:

[Address Book Lookup](#) (see page 301)
[Message Attribute Lookup](#) (see page 304)
[User Attribute Lookup](#) (see page 297)
[XML Attribute Lookup](#) (see page 306)

Data Lookup Syntax

For details about Data Lookup command syntax, see the following references.

More information:

[User Attribute Lookup Syntax](#) (see page 297)
[XML Attribute Lookup Syntax](#) (see page 307)
[Address Book Lookup Syntax](#) (see page 302)
[Message Attribute Lookup Syntax](#) (see page 304)

Data Lookup Commands and True-False Tests

A Data Lookup command is an individual setting within an email trigger. The command itself specifies one or more tests. Each test is a True or False statement that relates to an email characteristic. For example, a Data Lookup command may test whether any of the email recipients belong to a particular department. Or it may test whether an email is larger than, for example, 50KB. A Data Lookup command for this test follows:

```
msgattr WHERE msgsizekb > 50
```

If the test returns a True value, the Data Lookup command causes the trigger to activate. If you define a command with multiple tests, you can specify whether any or all of the test results must be True in order to activate the trigger.

For example, you can define a Message Attribute lookup command that activates a control trigger if the total message impact (the message size multiplied by the number for recipients) exceeds, for example, 1MB. If this returns a True value, the trigger activates to block the email or warn the user against sending it.

Likewise, you can define an Address Book lookup command that activates a control trigger if the test for any email recipient returns a True value. For example, you may want to prevent certain users sending emails to members of the Sales department. Here, for each targeted email, recipient tests return a False value if a recipient is not in Sales. If CA DataMinder detects any recipient who is in the Sales department, the Data Lookup test for that recipient returns a True value and the control trigger activates to block the email.

Add Data Lookup Commands to Control Triggers

To specify the Data Lookup Command trigger setting

1. Open the User Policy Editor and locate the email trigger that you want to change.
2. Display the trigger settings.
3. Edit the Data Lookup Command setting and type a command to exempt or target specific types of email. You can define simple or complex lookup commands, or combine multiple commands to target internal emails that meet a precise set of conditions.
4. Edit the Data Lookup Failure Mode setting. If the Data Lookup command cannot run, this setting determines whether or not the trigger activates. Choose an action from the list of available options. For example, choose 'Fire trigger' to specify that the trigger always activates if the Data Lookup command fails to run.

Or you can choose 'Block Event'. This simply blocks the email with an advisory dialog. If you block the email, you can configure the title and message in the advisory dialog; find the relevant settings in the System Settings, User Notifications policy folder.

Note: Data Lookup commands can fail to run if, for example, there is a syntax error or the computer is not connected to the network so Address Book details cannot be extracted from the Microsoft Exchange server. This last reason particularly affects laptop users.

More information:

[User Attribute Lookup Syntax](#) (see page 297)

[XML Attribute Lookup Syntax](#) (see page 307)

[Address Book Lookup Syntax](#) (see page 302)

[Message Attribute Lookup Syntax](#) (see page 304)

Data Lookup Failure Mode

The Data Lookup Failure Mode setting determines how to handle emails if the Data Lookup command cannot run. This can happen if, for example, there is a syntax error or the computer cannot connect to the Microsoft Exchange server to extract Address Book details. This last reason particularly affects laptop users.

If an email meets all the trigger criteria but the Data Lookup command cannot run, you can set the lookup failure mode to:

Fire trigger

The trigger is always activated.

Do not fire trigger

CA DataMinder ignores the email and the trigger does not activate.

Block event (client only)

Only available for outgoing emails. This option varies, depending on whether a CA DataMinder client agent or server agent is processing the email.

- If a client agent is processing the email, CA DataMinder always blocks the email with an accompanying notification message. This message is defined by the Terminate E-mail Processing settings. Find these settings in the System Settings, User Notifications folder.
- If a server agent is processing the email, CA DataMinder always activates the trigger. Note that the range of available control interventions is more limited for CA DataMinder server agents.

Data Lookup Commands and Included, Excluded and Ignored Lists

Data Lookup commands that use %sender%, %recipient%, %senderalias% or %recipientalias% variables are affected if the trigger uses an Included, Excluded or Ignored address list.

If a trigger uses an:

- **Included Addresses** list, these data lookup commands only evaluate included email addresses.
- **Excluded Addresses** list, these data lookup commands do not evaluate excluded email addresses.
- **Ignored Addresses** list, these data lookup commands do not evaluate ignored email addresses.

User Attribute Lookup

More information:

[User Attribute Lookup Syntax](#) (see page 297)

[Enable Regionalized Policy Engine Lookup](#) (see page 299)

[User Attribute Lookup Examples](#) (see page 300)

User Attribute Lookup Syntax

User Attribute lookup can detect e-mails sent to or from CA DataMinder users with specific account attributes. A syntax summary and brief examples are given below.

Before you can use User Attribute lookup commands, you must configure additional [policy settings](#) (see page 298).

Note: CA DataMinder triggers can also detect emails sent to or from non- CA DataMinder users by the absence of a specific user attribute.

Simple Commands

These commands test a simple True or False statement relating to a single user attribute of the email recipients or sender. For example, if a 'Team' attribute has been created for your organization, you can define a command to test whether any email recipients are members of a specific team. The syntax is:

```
userattr WITH <who> [labeled <fallguy>] WHERE <uservar> [labeled <offlimits>]  
  <stringoperator> <text>
```

The simple example below detects all outgoing emails where any of the recipients are members of the equity markets team:

```
userattr WITH any %recipient% WHERE Team IS "Equity Markets"
```

Complex Commands

More complex commands can include AND, OR and NOT operators to combine multiple True or False tests. For example, if 'Team' and 'Rank' attributes have been created for your organization, you can define a command to test whether an email's recipients include a manager in the equity markets team.

More information:

[Configure Policy Settings for User Attribute Lookup](#) (see page 298)

[<Stringoperator>](#) (see page 327)

[<Text>](#) (see page 330)

[Labeled <Fallguy>](#) (see page 318)

[Labeled <Offlimits>](#) (see page 320)

[<Type>](#) (see page 331)

Configure Policy Settings for User Attribute Lookup

Before you can use User Attribute lookup commands, you must configure settings in the user policy and machine policy.

Configure Email Address Mapping

Important! You must set up email address mappings before you can use User Attribute lookup commands.

In the machine policy, settings in the E-mail User Identification folder enable email triggers to map the recipients of an outgoing email (or the sender of an incoming email) onto CA DataMinder users. Triggers can then evaluate the lookup command, comparing the attributes of the recipients (or the sender of an incoming email) against the test criteria.

There are two alternative mapping methods. First, conversion expressions parse and extract the key address components to derive a CA DataMinder user name. Second, the database lookup method checks a customized user attribute to compare captured email addresses against known CA DataMinder user accounts. You set up your preferred mapping method in the machine policy. For details about email address mapping, see the *Platform Deployment Guide*.

Configure Lookup Timeouts

You can also specify timeouts for lookup commands in the user policy. These prevent emails being delayed unnecessarily if it is taking too long to retrieve the attribute details from the parent server. These timeouts are defined in the System Settings policy folder.

Enable Regionalized Policy Engine Lookup

You can tell the Policy Engine to only apply policy to an email if the sender is located in a specific region (user group). Regionalized Policy Engine Lookup introduces the %region% data lookup variable to the User Attribute Lookup family.

UserAttr WITH ANY %Sender% WHERE Wgn.GroupParent IS %region%

Follow these steps:

To enable this feature, create and set the registry key 'PERegion' on each regional Policy Engine:

SOFTWARE\ComputerAssociates\CA DataMinder\CurrentVersion\UserProcess

PERegion

Defines the region of the Policy Engine as a user group. Verify that all users in this region are in a single user group hierarchy.

Data Type: REG_SZ

Values: The syntax is same as the <Text> data lookup variable. Enclose search terms in {"double quotes with curly braces"}.

Example:

The administrator sets up "UK", "US," and "HK" user groups, and defines the PERegion key value of his three regional Policy Engines as follows:

```
PERegion {"UK"}
```

```
PERegion {"HK"}
```

```
PERegion {"US"}
```

The administrator uses the following lookup command:

```
UserAttr WITH ANY %Sender% WHERE Wgn.GroupParent IS %region%
```

In the following example, the sender is located in the UK:

1. If the %sender% group parent is that of Policy Engine region, and the sender belongs the user group "UK", then the lookup command returns TRUE.

The CMS puts this one copy of the event into the database.

2. All other regional Policy Engines have different values for PERegion.

The data lookup command returns FALSE and policy is not applied.

3. The iConsole shows one event.

Without Regionalized Policy Engine Lookup, the iConsole displays multiple events (one for each PE), and applies the same policy to senders in all regions.

More information:

[<Text>](#) (see page 330)

User Attribute Lookup Examples

These examples assume that the custom attributes 'Team' and 'Rank' have been defined for the CA DataMinder users in your organization.

- This example detects attempts to print or copy a file where the user is in the Equity Markets team:
userattr WITH %user% WHERE Team IS "Equity Markets"
- This example detects attempts to print or copy a file where the user is not a director:
userattr WITH %user% WHERE Rank IS NOT "director"
- This example detects attempts to print or copy a file where the user is in the Equity Markets team. If CA DataMinder detects such a user, that user's name and team are written to the %which_guy% and %proscribed_team% variables respectively. You can then incorporate these variables in a user notification message:
userattr WITH %user% labeled %which_guy%
WHERE Team labeled %proscribed_team% IS "Equity Markets"

The following email examples refer to emails sent internally within an organization. User Attribute lookup does not detect emails sent to or from external addresses.

- This example detects all outgoing emails where one or more recipients is in the Equity Markets team. If CA DataMinder detects such a recipient, that user's name and team are written to the %which_guy% and %proscribed_team% variables respectively. You can then incorporate these variables in a user notification message:

```
userattr WITH any %recipient% labeled %which_guy%  
WHERE Team labeled %proscribed_team% IS "Equity Markets"
```

- This example detects all outgoing emails where a recipient is a member of teams such as Equity Markets or Debt Markets:
userattr WITH any %recipient% WHERE Team CONTAINS ANY {"Equity","Debt"}
- This example detects all outgoing emails where recipients include any junior ranking staff (in this case, 'Non-officers'):
userattr WITH any %recipient% WHERE Rank CONTAINS ALL {"non","officer"}
- This example detects all outgoing emails that do not include a director in the list of recipients:
userattr WITH all %recipient% WHERE Rank EXCLUDES "director"
- This example detects all outgoing emails where the recipient list excludes an executive director in the Equity Markets team. That is, the command returns a True value (and activates the control trigger) if no such recipient is detected.

Note the NOT operator! The NOT operator ensures that if an executive director in the Equity Markets team is detected, the command returns a False value (and the trigger does not activate). The mandatory keyword ensures that, if no Rank is specified, the data lookup command fails and invokes the Data Lookup Failure Mode.

```
userattr WITH all %recipient%  
WHERE  
  (Team IS NOT "Equity Markets")  
AND  
  (mandatory Rank IS NOT {"executive","director"})
```

- This example combines Message Attribute and User Attribute lookup commands to detect emails sent to members of any securities team where the total message impact exceeds 1MB:
(msgattr WHERE msgimpactkb > 1000) AND (userattr WITH any %recipient%
WHERE Team CONTAINS "Securities")

Address Book Lookup

More information:

[Address Book Lookup Syntax](#) (see page 302)

[Address Book Lookup Examples](#) (see page 303)

Address Book Lookup Syntax

Address Book lookups can detect emails with specific sender or recipient characteristics sent internally within an organization. It can only detect emails sent to or from addresses in the Global Address List. Syntax summaries and brief examples are given below.

Simple Commands

These commands test a simple True or False statement relating to a single Outlook Address Book property of the email recipients or sender. For example, a command may test whether any email recipients are members of specific email distribution lists. The syntax is:

```
mapi WITH <who> [labeled <fallguy>] WHERE <uservar> [labeled <offlimits>] <string operator> <text>
```

The simple example below detects all outgoing emails where any of the recipients belong to the Sales or Marketing departments:

```
mapi WITH any %recipient% WHERE Department IS ANY {"Sales","Marketing"}
```

Complex Commands

More complex commands can include AND, OR and NOT operators to combine multiple True or False tests. For example, a command may test whether any email recipients work in the London office and are in the Sales department.

Address Book Lookup Examples

These examples refer to emails sent internally within an organization. Address Book lookup does not detect emails sent to or from external addresses. These examples illustrate the various operator combinations in an Address Book lookup command.

- The example below detects all outgoing emails where one or more recipients is in the Sales department. If CA DataMinder detects such a recipient, that user's name and department are written to the %which_guy% and %proscribed_dept% variables respectively. You can then incorporate these variables in a user notification message:

```
mapi WITH any %recipient% WHERE Department IS ANY {"Sales","Marketing"}
```

- The example below detects all outgoing emails unless one or more recipients is in the London or Manchester offices:

```
mapi WITH all %recipient% WHERE Office IS NOT ALL {"London","Manchester"}
```

- The example below detects all incoming emails where the sender is a member of the Executive Management mail group:

```
mapi WITH %sender% WHERE MemberOf is "Executive" "Management"
```

- The example below detects all outgoing emails where one or more recipients has a hire date of 2001. (In this example, Address Book custom attribute 3 is set to an employee's hire date.)

```
mapi WITH any %recipient% WHERE ExtensionAttribute3 CONTAINS "2001"
```

- The example below detects all outgoing emails that do not include a supervisor in the list of recipients:

```
mapi WITH all %recipient% WHERE Title IS NOT "Supervisor"
```

- The example below detects all outgoing emails that do not include a supervisor or team leader in the list of recipients. The command returns a True value (and activates the control trigger) unless a supervisor or team leader is included in the To, Cc or Bcc lists:

```
mapi WITH all %recipient% WHERE Title IS NOT "Supervisor"
```

- The example below detects all outgoing emails where the recipient list excludes a member of the Compliance Team mail group in the London office. That is, the command returns a True value (and activates the control trigger) if no such recipient is detected.

Note the NOT operator! This ensures that if any member of the London Compliance Team is detected, the command returns a False value (and the trigger does not activate).

```
mapi WITH all %recipient%  
  WHERE NOT ((MemberOf CONTAINS ALL {"Compliance","Team"})  
    AND (Office IS "London"))
```

- The example below combines Message Attribute and Address Book lookup commands to detect emails sent to the Santiago office where the total message impact exceeds 5MB:
(msgattr WHERE msgimpactkb > 5000) AND (mapi WITH any %recipient% WHERE Office IS "Santiago")
- The example below tests the Company attribute of the user, but specifies it by its MAPI numerical code:
mapi WITH any %recipient% WHERE MAPIID0x3A16 IS "Unipraxis"

Message Attribute Lookup

More information:

[Message Attribute Lookup Syntax](#) (see page 304)

[Message Attribute Lookup Examples](#) (see page 305)

Message Attribute Lookup Syntax

Message Attribute lookups can be used to access information contained in an email that is not accessible through any other trigger. For example, they can detect whether emails are DRM-protected, digitally signed or encrypted. They can also detect outgoing emails based on their potential impact on network traffic.

Note: Message Attribute lookup exemptions are not appropriate for the 'Sender' incoming email trigger.

Syntax summaries and brief examples are given below.

Simple Commands

These commands test a simple True or False statement relating to a message attribute. For example, a command may test whether the number of recipients exceeds the maximum permitted, or whether the total message impact (the message size multiplied by the number for recipients) exceeds a maximum threshold. The syntax is:

```
msgattr WHERE <msgvar> <numericoperator> <msgvalue>
```

The simple example below detects all outgoing emails where the total message impact exceeds 1MB:

```
msgattr WHERE msgimpactkb > 1000
```


Complex Commands

You can also combine multiple commands using AND, OR and NOT operators. For example, you can combine two commands to test, first, whether an individual message exceeds a maximum size and, second, whether it is addressed to, for example, more than ten recipients.

More information:

[<Stringoperator>](#) (see page 327)

[<Text>](#) (see page 330)

[<msgvalue>](#) (see page 321)

[<Numericoperator>](#) (see page 327)

[<Type>](#) (see page 331)

[<msgvar>](#) (see page 322)

Message Attribute Lookup Examples

These examples illustrate the various operators in Message Attribute lookup commands.

- The example below detects all DRM-protected emails:
`msgattr WHERE isDRMProtected`
Note: DRM-protected emails cannot be detected by the CA DataMinder Notes endpoint agent or Domino server agent.
- The example below detects all digitally signed emails:
`msgattr WHERE isSigned`
- The example below detects all encrypted emails:
`msgattr WHERE isEncrypted`
- The example below detects all outgoing emails bigger than 50 KB:
`msgattr WHERE msgsizekb > 50`
- The example below exempts all meeting requests and responses to meeting requests:
`msgattr WHERE messageclass IS ANY
("IPM.Schedule.Meeting.Request", "IPM.Schedule.Meeting.Resp.*")`
- The example below detects all outgoing emails where the total message impact exceeds 1 MB:
`msgattr WHERE msgimpactkb > 1000`
- The example below detects all outgoing emails with 10 or more recipients:
`msgattr WHERE recipnum >= 10`
- The example below detects all outgoing emails sent to more than ten internal addresses:
`msgattr WHERE internalrecipnum > 10`

- The example below detects all outgoing emails sent to more than one external addresses:
`msgattr WHERE externalrecipnum > 1`
- The example below detects all outgoing emails from specific users at Unipraxis to any user at CA.
`msgattr WHERE (%sender% IS ANY {"srimmel@unipraxis.com", "lstee@unipraxis.com"})
AND (%recipient% labeled %which_recip% IS "@ca.com")`
- The example below detects all outgoing emails sent to 20 or more recipients in the To list:
`msgattr WHERE tonum >= 20`
- The example below detects all outgoing emails with no recipients in the Cc list:
`msgattr WHERE ccnum = 0`
- The example below detects all outgoing emails that do not have one recipient in the Bcc list:
`msgattr WHERE bccnum <> 1`
- The example below detects all outgoing emails where the total number of To and Cc recipients is over 20:
`msgattr WHERE toccnum > 20`
- The example below detects emails where the importance 'is not low'. In effect, it excludes emails with low importance and detects emails with normal or high importance:
`msgattr where importancelevel <> 0`
- The example below detects confidential emails with high importance:
`msgattr where sensitivitylevel = 3 and importancelevel = 2`
- The example below detects urgent emails:
`msgattr where prioritylevel = 1`

XML Attribute Lookup

XML Attribute lookups can be used to detect metadata attributes of events. This metadata is stored in XML format. This allows policy triggers to access event information that is not accessible through any other trigger. Syntax summaries and brief examples are given below.

What Is XML Metadata?

XML metadata contains ancillary information about the item itself (for example, when a file was created or an x-header inserted into an Internet Mail).

This XML metadata is not the same as the event metadata stored by CA DataMinder on the CMS. This event metadata contains details about the CA DataMinder event (for example, the event capture date, participants, and trigger details).

For full schema details, see the *Data Lookup XML Schema Reference Guide*.

More information:

[XML Attribute Lookup Syntax](#) (see page 307)

[XML Attribute Lookup Examples](#) (see page 309)

[XML Metadata Examples](#) (see page 311)

XML Attribute Lookup Syntax

Simple Commands

These commands test a simple True or False statement relating to an XML attribute. For example, a lookup command may test the file name of an imported file. The syntax is:

```
xmllattr [WITH <xpath>] [labeled <offlimits>] WHERE <xpath> [labeled <offlimits>]  
<stringoperator|numericoperator> <attribvalue>
```

Where:

<xpath> specifies an element within the XML schema for event metadata.

<attribvalue> must be enclosed in double quotes. The simple example below detects all files created on or after 10am, 18 May 2009 UTC (equivalent to 6am EST during daylight saving time):

```
xmllattr WHERE apm/event/file/created >= "2009-05-18T10:00:00"
```

Note: Be aware that dates and times are stored as UTC.

WITH and WHERE Statements

In a simple xmlattr lookup command, the WHERE statement locates and identifies the actual file attribute whose value is to be tested.

But xmlattr lookup commands can optionally include a WITH statement to locate the attributes, allowing the use of simplified WHERE statements to identify which attributes to test. This is useful if you want to test multiple attributes. For example, the filename and size attributes are both located on the *file* XML node; the command below tests for MS Word documents over 1Mb:

```
xmlattr WITH apm/event/file WHERE (filename IS "*.doc") AND (size > 1048576)
```

Property Sets

The metadata for a file can include one or more property sets. A property set is a collection of related file properties. The <xpath> syntax for referencing a property is: apm/event/file/property_set[@name=<set name>]/property[@name=<property name>]

Where <set name> and <property name> must be enclosed in double quotes. For example:

- Microsoft Word documents include a 'Summary' property set that includes 'TotalEditingTime' and 'WordCount' properties. The following command causes a trigger to fire when the word count in a document is greater than 10,000:

```
xmlattr WHERE  
apm/event/file/property_set[@name="Summary"]/property[@name="WordCount"] >  
10000
```

- You may want to identify specific items when the FSA scans items in Exchange Public Folders. These items include an 'Exchange' property set that contains a 'MessageClass' property.

The following command causes a trigger to fire when the FSA detects a note item. As a result, the FSA *includes* these items in the scan:

```
xmlattr WHERE  
apm/event/file/property_set[@name="Exchange"]/property[@name="MessageClass"]  
= "IPM.Note"
```

Conversely, the following command prevents a trigger from firing when the FSA detects appointment or meeting request items. As a result, the FSA *excludes* these items from the scan:

```
xmlattr WHERE apm/event/file/property_set[@name="Exchange"]/property  
[@name="MessageClass"] IS NOT "IPM.Appointment"
```

Note: IPM.Appointment item types include appointments *and* meeting requests.

The other main items in Exchange Public Folders are contacts and tasks. The 'MessageClass' property for a contact is IPM.Contact. The 'MessageClass' property for a task is IPM.Task.

Complex Commands

More complex commands can include WITH, AND, OR and NOT operators to combine multiple True or False tests. For example, a command may look for files created after 14 May and before 18 May.

Dates and Times Stored in UTC

CA DataMinder stores all date and time metadata in UTC (Coordinated Universal Time). Your xmlattr lookup commands must therefore specify UTC dates and times.

For example, a file is created at 11am, 18 May 2009 in New York during daylight saving time (UTC-4). Therefore, the data lookup command to find this file must specify a 3pm file creation time:

```
xmlattr WHERE apm/event/file/created >= "2009-05-18T15:00:00"
```

Note:The iConsole and Data Management console convert dates and times back to local time when displaying the associated events.

More information:

[XML Attribute Lookup Examples](#) (see page 309)

[XML Metadata Examples](#) (see page 311)

[<Attribvalue>](#) (see page 317)

[<Xpath>](#) (see page 337)

XML Attribute Lookup Examples

These examples illustrate the various operator combinations in XML Attribute lookup commands.

Detecting Email X-headers

- The example below detects emails containing an x-header named 'x-vpm-state'
`xmlattr WHERE apm/event/email/header/item[@name='x-vpm-state'] IS ""`
- The example below detects emails containing an x-header named 'x-vpm-state' where the x-header value is set to 'sensitive'.
`xmlattr WHERE apm/event/email/header/item[@name='x-vpm-state'] IS "sensitive"`

- The example below detects emails containing an x-header named 'x-vpm-state' where the x-header value is set to 'public', and excludes these emails from policy processing. That is, the trigger does not fire.
`NOT (xmlattr WHERE apm/event/email/header/item[@name='x-vpm-state'] IS "public")`

Detecting File Attributes

- The example below detects all imported files smaller than 10 KB. Note that the file size attribute is measured in bytes, not KB.
`xmlattr WHERE apm/event/file/size < 10240`
- The example below tests the path attribute to detect all files imported from the \Tips folder on the machine UX-RIMMEL:
`xmlattr WHERE apm/event/file/path IS "\\UX-RIMMEL\Personal\Tips"`
Note: You do not need to specify a UNC path. You can also specify a local drive path if your policy engine is running on the same machine as the source folder.
- The example below detects all imported files that were modified between 21 and 25 May 2007:
`xmlattr WHERE (apm/event/file/modified >= "2007-05-21") AND (apm/event/file/modified < "2007-05-26")`
Note: All date and time metadata is stored in UTC (Coordinated Universal Time) on the CMS. Your xmlattr lookup commands must therefore specify UTC dates and times.
- Many files, particularly Microsoft Word documents, include an Author property. CA DataMinder always attempts to identify and store this as an attribute in the file event's metadata. This example detects all files where the author name includes the strings Rimmel or Steel:
`xmlattr WHERE apm/event/file/author CONTAINS ANY {"Rimmel","Steel"}`
- The example below checks the 'Security' property in Microsoft Word documents. This property is in the 'Custom' property set. Here, the xmlattr lookup command detects documents that are not marked as 'Confidential':
`WHERE apm/event/file/property_set[@name="Custom"]/property[@name="Security"] IS NOT "Confidential"`
- The example below uses a WITH statement to check the 'Security' and 'Status' properties in Microsoft Word documents. Status, like Security in the previous example, belongs to the 'Custom' property set.

Here, the xmlattr lookup command detects documents marked as 'Confidential' and whose status is 'Approved':
`WITH apm/event/file/property_set[@name="Custom"] WHERE ([property[@name="Security"]] IS "Confidential") AND ([property[@name="Status"]] IS "Approved")`
- The example below simply checks whether a 'Custom' or 'Version' property set is defined in the XML metadata:
`WHERE apm/event/file/property_set/@name IS ANY {"Custom","Version"}`

More information:

[XML Attribute Lookup Syntax](#) (see page 307)

[XML Metadata Examples](#) (see page 311)

XML Metadata Examples

The following sections show example XML metadata hierarchies for Word documents, printed documents, and email x-headers.

XML Metadata for Word Documents

An example XML hierarchy of metadata for a Microsoft Word document is shown below.

```
<?xml version="1.0"?>
<apm schema_version="1" xmlns="http://www.orchestria.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.orchestria.com xmleventattributes.xsd">
  <event>
    <file>
      <host>UX-RIMMEL</host>
      <filename>Sales_2007_Q1.doc</filename>
      <path>\\UX-RIMMEL\Personal\Tips</path>
      <created>2007-05-13T19:26:32</created>
      <accessed>2007-05-17T08:12:44</accessed>
      <modified>2007-05-16T21:05:54</modified>
      <size>41984</size>
      <title>Unipraxis Sales Q1 2007</title>
      <subject>Sales Revenue</subject>
      <author>Spencer Rimmel</author>
      <property_set name="Summary">

        <property prop_id="1" name="TotalEditingTime" type="xs:string">01:26:35</property>
        <property prop_id="2" name="WordCount" type="xs:string">824</property>

        <property prop_id="3" name="LastPrinted" type="xs:string">2007-05-17T08:14:36</property>
      </property_set>
      <property_set name="Custom">

        <property prop_id="1" name="Security" type="xs:string">Confidential</property>
        <property prop_id="2" name="Status" type="xs:string">Approved</property>
      </property_set>
    </file>
  </event>
</apm>
```

As far as possible, CA DataMinder attempts to fully populate the file metadata with relevant attributes. However, the range of available metadata items will vary by file type and file source. For example, if a third-party application passes the file data to CA DataMinder in the form of a byte stream, rather than providing CA DataMinder with access to the original file, then policy triggers can test for file attributes included in the byte stream. That is, CA DataMinder cannot independently identify or determine any missing attributes.

More information:

[XML Metadata for Printed Documents](#) (see page 312)

[XML Metadata for Email X-headers](#) (see page 313)

XML Metadata for Printed Documents

An example XML hierarchy of metadata for a printed document is shown below.

```
<?xml version="1.0"?>
<apm schema_version="1" xmlns="http://www.orchestria.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.orchestria.com xmleventattributes.xsd">
  <event>
    <file>
      <host>130.119.46.229</host>
      <device type="printer" local="false" server="UK-PRINTSVR"
        location="Taunton, Mezzanine">PrintMaster 2000</device>
      <application>WINWORD.EXE</application>
      <created>2010-04-19T10:54:42.237</created>
      <size>30276</size>
      <subject>Microsoft Word – Q2 Strategy.docx </subject>
      <property_set name="Print">
        <property name="Pages" type="xs:unsignedInt">1</property>
        <property name="Comment" type="xs:string"/>
        <property name="Paper" type="xs:string">Letter 8 1/2 x 11 in</property>
      </property_set>
      <stream name="Page 1.emf">
        <size>30276</size>
        <type>data</type>
      </stream>
      <hash type="sha-256">7EBFC9D20069500208FD5B144B9F73F58A3705F
        F5C293B1943E35C852BD683AD</hash>
    </file>
  </event>
</apm>
```

As far as possible, CA DataMinder attempts to fully populate the event metadata with relevant attributes. However, the range of available metadata items will vary. For example, location details may not have been configured for the printer.

More information:[XML Attribute Lookup Syntax](#) (see page 307)[XML Attribute Lookup Examples](#) (see page 309)

XML Metadata for Email X-headers

An example of XML metadata for email is shown below. This shows a single x-header named x-vpm-state and with a value of 'sensitive'.

```
<?xml version="1.0" encoding="UTF-8"?>
<apm schema_version="1" xmlns="http://www.orchestria.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.orchestria.com xmleventattributes.xsd">
  <event>
    <email>
      <header type="x-header">
        <item name="x-vpm-state" type="xs:string">sensitive</item>
      </header>
    </email>
  </event>
</apm>
```

More information:[XML Attribute Lookup Syntax](#) (see page 307)[XML Attribute Lookup Examples](#) (see page 309)

Command Variables

Data Lookup commands support the following variables.

More information:

[General Guidelines](#) (see page 314)

[<Who>](#) (see page 314)

[<Attribvalue>](#) (see page 317)

[Labeled <Fallguy>](#) (see page 318)

[Labeled <Offlimits>](#) (see page 320)

[<msgvalue>](#) (see page 321)

[<msgvar>](#) (see page 322)

[<Numericoperator>](#) (see page 327)

[<Stringoperator>](#) (see page 327)

[<Text>](#) (see page 330)

[<Type>](#) (see page 331)

[<Uservar>](#) (see page 332)

[<Xpath>](#) (see page 337)

General Guidelines

In data lookup commands, syntax is not case-sensitive, and line breaks and extra spaces are ignored.

Syntax is case-insensitive

All syntax elements and variables are case-insensitive. This includes <text> search terms in double quotes. For example, if you want to detect emails sent to the Sales department, then you can set <text> to "Sales", "sales" or "SALES". All will return a True value if CA DataMinder detects a member of the Sales team.

Command layout

When entering Data Lookup commands in the Policy Editor, you can add line breaks and extra spaces to make commands easier to read and maintain, for example:

```
(msgattr WHERE msgimpactkb > 1000)
AND
(userattr WITH any %recipient% WHERE Team CONTAINS "Securities")
```

<Who>

For userattr, msgattr, and mapi commands.

<who> determines whether the email recipients or the sender are tested for characteristics that match the Data Lookup criteria. They are used with <stringoperator> to test for messages from specific senders, or messages sent to specific recipients.

The following <who> formats are supported:

%user%

(Only applicable to 'print or save' Data In Motion triggers.)

You can use 'with %user%' lookup commands in Data In Motion triggers invoked by the Client File System Agent (CFSA) or Client Print System Agent (CPSA). That is, use these lookup commands in triggers that detect files being printed or files being copied or saved to removable devices and network locations.

The Data In Motion trigger activates if the user's CA DataMinder account attribute matches the User Attribute Data Lookup criteria. The following lookup commands use IS and IS NOT operators to demonstrate a positive or negative inference respectively:

```
userattr with %user% where Department IS "Sales"
```

```
userattr with %user% where Rank IS NOT "Director"
```

Note: 'With %user%' lookup commands are *not* supported in Data In Motion triggers invoked by the CA DataMinder Network agent or ICAP agent. That is, you cannot use these lookup commands to detect files leaving your corporate network for the Internet, or files arriving from the Internet (such as file uploads or FTP transfers).

%recipient%

The trigger activates if the user attributes, Address Book properties, e-mail addresses, or display names for the recipients match the Data Lookup criteria. Specifically, there must be a match for any recipient, or every recipient, depending on whether the ANY or ALL operator is used.

Data lookup commands that compare strings have either a positive or negative inference. The following lookup commands use IS and IS NOT operators to demonstrate a positive or negative inference respectively:

```
mapi with ANY %recipient% where department IS "Sales"
```

```
mapi with ALL %recipient% where department IS NOT "Sales"
```

To simplify matters, you can use %recipient% without actually specifying ANY or ALL. For example, in the 'positive' mapi command, there is an implicit ANY before %recipient%:

```
mapi with %recipient% where department IS "Sales"
```

In the 'negative' mapi command, there is an implicit ALL before %recipient%:

```
mapi with %recipient% where department IS NOT "Sales"
```

any %recipient%

The trigger activates if the user attributes or Address Book properties for any of the recipients match the Data Lookup criteria. If none of the recipients have matching user attributes or Address Book properties, the trigger does not activate.

all %recipient%

The trigger activates only if the user attributes or Address Book properties of every recipient match the Data Lookup criteria. If any of the recipients have user attributes or Address Book properties that do not match the Data Lookup criteria, the trigger does not activate.

%sender%

Only the sender's user attributes or Address Book properties can activate the trigger.

%sentonbehalf%

You can use Data Lookup commands to trigger policies on Sent-on-Behalf-of users.

Note: Previous releases of CA DataMinder considered the delegate user as Sender, and applied the policy to the *delegate*. 'Sent-on-behalf-of' users are now detected as Senders by default, and policy is applied to them.

Example: User A allows Delegate B to send emails on his behalf. Although the email sender is Delegate B, policy is applied to User A using the %sentonbehalf% attribute.

UserAttr WITH %sentonbehalf% WHERE Wgn.GroupParent IS {"UK"}

Note: These formats can all be used in conjunction with <fallguy> subexpressions.

Internal and external recipients

Internal email addresses and, by inference, external addresses are defined by the Internal E-Mails setting in the Definitions folder of the user policy. The mechanism for matching email addresses against internal address patterns is the same as that used by CA DataMinder to match email addresses against lists of addresses defined in the capture or control triggers of a user policy.

More information:

[Address Book Lookup](#) (see page 301)

[Message Attribute Lookup](#) (see page 304)

[User Attribute Lookup](#) (see page 297)

<Attribvalue>

For xmlattr commands only.

<attribvalue> is the value of the XML metadata attribute you are testing. It can be a text value, a number, or a date.

Text

For example, if <xpath> specifies the title attribute, then set <attribvalue> to 'Sales Q1 2007' to detect documents whose Title property includes that term:

```
WHERE apm/event/file/title CONTAINS "Sales Q1 2007"
```

If <xpath> specifies an x-header in an email, you can set <attribvalue> to the value of the x-header. For example, this lookup tests whether the 'x-vpm-state' x-header is set to 'sensitive':

```
xmlattr WHERE apm/event/email/header/item[@name='x-vpm-state'] IS "sensitive"
```

Number

For example, if <xpath> specifies the file size attribute, then set <attribvalue> to 1,048,576 to detect files with a minimum size of 1 MB. Note that the file size attribute is measured in bytes, not KB or MB:

```
WHERE apm/event/file/size >= 1048576
```

Note: You do not need to enclose numeric values in double quotes.

Date

For example, if <xpath> specifies the 'date modified' attribute, then to detect all imported files that have been modified since 21 May 2007, set <attribvalue> to the following.

```
WHERE apm/event/file/modified >= "2007-05-21"
```

Note that dates must take the following format:

```
2007-05-21T18:00:00
```

If the time element (T18:00:00 in the example above) is omitted, the time defaults to midnight. For example:

2007-05-21 is equivalent to:

```
2007-05-21T00:00:00
```

Properties in a property set

<attribvalue> can also test the value of properties in a file's 'property set' (if included in the file's XML metadata). In effect, property sets are collections of related file attributes.

For example, the 'Version' property set for an executable file typically contains properties such as Company, File Version and Language. A lookup command to test the value of a property takes the following format:

```
WHERE apm/event/file/property_set[@name="Version"]  
      /property[@name="Language"] IS "English"
```

Similarly, a Microsoft Word document can include a 'Custom' property set, which can include any custom properties defined for that document. For example, an organization may use 'Security' and 'Status' custom properties to define a document's audience and to indicate whether the document has been approved. A lookup command to test these custom properties takes the following format:

```
WITH apm/event/file/property_set[@name="Custom"]  
    WHERE (property[@name="Security"] IS "Public")  
    AND (property[@name="Status"] IS "Approved")
```

In all cases, the @name property identifier must be enclosed in square brackets.

More information:

[<Xpath>](#) (see page 337)

[XML Metadata for Word Documents](#) (see page 311)

[XML Attribute Lookup](#) (see page 306)

Labeled <Fallguy>

For userattr and mapi commands only.

labeled <fallguy> is an optional subexpression that you can use to identify the e-mail recipient (or sender) for whom the data lookup command returned a True value and who, as a consequence, caused the control trigger to activate. The email address of this recipient (or sender) is assigned to the <fallguy> variable for inclusion in a user notification message.

This is especially useful if an e-mail is sent to lots of people, but only a small number of these are on the list of unauthorized recipients. <fallguy> permits you to identify these unauthorized recipients in a notification dialog, which in turn enables the sender to remove them from the addressees before resending the email.

Variable names

<fallguy> is a variable name chosen by you. Like all user notification variables, it must be enclosed in percent marks. You must not choose a variable name already used by CA DataMinder. One way to ensure your chosen variable name is acceptable is to include your company in the variable name. For example:

```
%XYZ_interdicted_user%
```

IS example

<fallguy> subexpressions are most easily understood in terms of data lookup commands that use an IS operator. In the example below, if an unauthorized recipient in the Equity Markets team causes a control trigger to activate, the address of that recipient is written to the %XYZ_interdicted_users% variable:

```
userattr WITH all %recipient% labeled %XYZ_interdicted_users% WHERE Team IS "Equity Markets"
```

For example, a user attempts to send an e-mail to various people including unauthorized recipient Frank Schaeffer. %XYZ_interdicted_users% is therefore set to 'Frank Schaeffer' or fschaeffer@unipraxis.com. (Where possible, <fallguy> returns the user's e-mail display name.)

If multiple unauthorized recipients are detected, the Data Lookup command writes all of them to %XYZ_interdicted_users%. These are displayed in the notification dialog as a comma-separated list:

```
fschaeffer@unipraxis.com,srimmel@unipraxis.com
```

IS NOT example

If you use an IS NOT operator in a data lookup command, <fallguy> works as normal and returns the e-mail address of every recipient for whom the data lookup command returned a True value. But you need to remember that the command logic is reversed!

For example, the command below returns a True value if none of the recipients are directors. In this case, the address of each recipient is written to the variable %XYZ_renotify_these_guys% (because in each case, the recipient is not a director and so the test returns a True value):

```
userattr WITH all %recipient% labeled %XYZ_renotify_these_guys% WHERE Rank IS NOT "director"
```

If none of the recipients are directors, then %XYZ_renotify_these_guys% will contain a list of addresses for all the intended recipients, for example:

```
fschaeffer@unipraxis.com,srimmel@unipraxis.com
```

More information:

[Address Book Lookup](#) (see page 301)

[User Attribute Lookup](#) (see page 297)

Labeled <Offlimits>

For userattr and mapi commands only.

labeled <offlimits> is an optional subexpression that you can use to identify the Address Book property or user attribute for which the data lookup command returned a True value and, as a consequence, caused the control trigger to activate. The property or attribute is assigned to the <offlimits> variable for inclusion in a user notification message.

This is especially useful if an e-mail is sent to lots of recipients, but only a small number of these have attributes or properties that disqualify them from receiving the e-mail. <offlimits>, when used in conjunction with <fallguy>, permits you to identify these recipients and highlight their disqualifying property or attribute. In turn, this enables the sender to remove them from the addressees before resending the e-mail.

Variable names

<offlimits> is a variable name chosen by you and, like all user notification variables, must be enclosed in percent marks. You must not choose a variable name already used by CA DataMinder. For example, one way to ensure your chosen variable name is acceptable is to include your company in the variable name. For example:

%XYZ_taboo_team%

For details about incorporating <offlimits> variables into a user notification message.

IS example

<offlimits> subexpressions are most easily understood in terms of data lookup commands that use an IS operator. In the example below, e-mails sent to members of certain teams (Equity Markets, Debt Markets or Securities Services) cause a control trigger to activate. For each 'disqualifying' recipient, their team name is written to the variable %XYZ_taboo_team%:

```
userattr WITH any %recipient% WHERE Team labeled %XYZ_taboo_team% IS ANY {"Equity Markets", "Debt Markets", "Securities Serv"}
```

For example, if a user attempts to send an e-mail to members of the Equity Markets team. %XYZ_taboo_team% is set to 'Equity Markets'. Likewise, if multiple unauthorized recipients are detected, the Data Lookup command writes all of their teams to %XYZ_taboo_team%. These are displayed in the notification dialog as a comma-separated list:

Equity Markets,Debt Markets,Securities Services

IS NOT example

If you use an IS NOT operator in a data lookup command, <offlimits> works as normal and returns the attribute or property of every recipient for whom the data lookup command returned a True value. But you need to remember that the command logic is reversed!

For example, the command below returns a True value if none of the recipients are directors. In this case, the actual rank of each recipient is written to the variable %XYZ_too_junior% (because in each case, the recipient is not a director and so the test returns a True value):

```
userattr WITH all %recipient% WHERE Rank labeled %XYZ_too_junior% IS NOT "director"
```

For example, if none of the recipients are directors then %XYZ_too_junior% will contain a list of the ranks that were detected, for example:

```
Intern,Management trainee,Non-officer
```

More information:

[Address Book Lookup](#) (see page 301)

[User Attribute Lookup](#) (see page 297)

<msgvalue>

For msgattr commands only.

<msgvalue> is always entered as a number.

It defines the threshold for a particular message attribute. For example, to specify a maximum permitted message size of 25MB, set <msgvalue> to 25600:

```
WHERE msgsizekb >= 25600
```

Note: Numbers are always extracted as integers. For example, 25.5 is truncated to 25.

More information:

[Message Attribute Lookup](#) (see page 304)

<msgvar>

For msgattr commands only.

<msgvar> represents the message attribute that you want to test. The following operators are supported:

Protected content values

Use these values to detect emails with protected content. Unlike most <msgvar> values, these take no comparison operator (such as > or <). They can be incorporated into complex commands to precisely target specific examples of emails with protected content.

isDRMProtected

This value returns True if an email is DRM-protected. or example:

```
msgattr WHERE isDRMProtected
```

Using this lookup value, CA DataMinder can detect DRM-protected emails that have been encrypted using Microsoft Windows Rights Management Services (RMS). RMS technology can be used to restrict the ways in which employees can use corporate emails, Word documents, and Web pages.

Note: DRM-protected emails cannot be detected by the CA DataMinder Notes endpoint agent or Domino server agent.

isSigned

This value returns True if an email is digitally signed.

This allows you, for example, to block or warn against sending emails if they do not have a digital signature, but exempt them if they are digitally signed.

isEncrypted

This value returns True if an email is encrypted.

This allows you, for example, to block or warn against sending emails if they are not encrypted, but exempt emails that are encrypted.

Message class values**messageclass**

This value returns the message class. This allows you to exclude specific categories of email such as meeting requests or read receipts. Common message classes that you can test for include:

IPM.Note

This is the standard message class for Outlook emails. Nearly all Outlook emails have this messageclass. To avoid burdening the CMS database with unnecessary data, the message class is not stored when it is simply 'IPM.Note'.

IPM.Schedule.Meeting.Request

This is the message class for meeting requests. The corresponding classes for 'Accept', 'Decline' and 'Tentative' invitee responses are:

IPM.Schedule.Meeting.Resp.Pos

IPM.Schedule.Meeting.Resp.Neg

IPM.Schedule.Meeting.Resp.Tent

IPM.TaskRequest

Task request.

REPORT.IPM.Note.DR

Delivery receipt.

REPORT.IPM.Note.IPNRN

Read receipt.

Numeric values: size (KB), recipients, domains

Use these values in conjunction with <numericoperator> to detect emails with specific numeric attributes. For example, these values can count the number of recipients or calculate the total network impact (in terms of KBs of data sent).

msgsizekb

Message size, including attachments (in kilobytes).

Note: This attribute is useful for blocking large emails. For example, preventing someone from sending a 5 MB email. The calculation methods used may not be accurate enough for blocking emails with a smaller impact.

For example, to detect all outgoing emails bigger than 5 MB:

```
msgattr WHERE msgsizekb > 5000
```

msgimpactkb

Total message impact (in kilobytes sent), calculated as:

Message size * No. of recipients

Note: This attribute is useful for blocking large emails. For example, preventing someone from sending a 5 MB email to 100 recipients. The calculation methods used may not be accurate enough for blocking emails with a smaller impact.

recipnum

Number of recipients

internalrecipnum

Number of internal recipients.

externalrecipnum

Number of external recipients.

tonum

Number of 'To' recipients. For example:

```
msgattr WHERE tonum >= 10
```

ccnum

Number of 'CC' recipients

bccnum

Number of 'BCC' recipients

toccnum

Number of 'To' and 'CC' recipients

domainnum

Number of unique domains in recipient list.

externaldomainnum

Number of unique external domains in recipient list. This domain count is based only on external recipients; see the following section for details about external recipients.

Numeric values: for blank emails or missing attachments

These attributes can detect poorly written emails. For example, an email with a blank Subject field, no body text, or without a mandatory attachment.

subjectlen

Number of characters in the Subject line, excluding any leading or trailing spaces. .
For example:

```
msgattr WHERE subjectlen = 0
```

normalizedsubjectlen

Number of characters in the 'normalized' Subject line, excluding any leading or trailing spaces.

A 'normalized' Subject line is one where prefixes such as RE: and FW: have been removed.

bodylength

Number of characters in the mail body text, excluding any leading or trailing spaces.

attachmentnum

Number of attachments.

Numeric values: email importance, sensitivity and priority

Email applications such as Microsoft Outlook allow senders to assign importance and sensitivity to emails. Some applications, such as Lotus Notes, also allow senders to assign a delivery priority. These <msgvar> values allow you to test emails for these attributes.

These are numeric attributes, with zero representing the lowest level of significance. You can test for individual levels of significance or a range of significance.

importancelevel

Tests email importance levels, where:

0=Low

1=Normal (This is the default level.)

2=High

sensitivitylevel

Tests email sensitivity, where:

0=None or not set. (This is the default level.)

1=Personal

2=Private

3=Confidential or Company-confidential

prioritylevel

Tests email delivery priority, where:

0=Low or Non-urgent

1=Normal (This is the default level.)

2=High or Urgent

<who> variables: %sender% and %recipient%

In addition to the <msgvar> values listed above, you can also use <who> variables such as %sender% and %recipient% in msgattr lookup commands.

These allow you to combine standard message attribute test (for example, recipient counts or checking for protected-content) with tests for specific senders or recipients. for example:

```
msgattr WHERE isEncrypted AND %sender% IS "srimmel@unipraxis.com"
```

Note: Results from these string values depend on the expansion of the email, which in turn is determined by the machine policy setting Perform LDAP directory lookups? and the user policy setting Retrieve Full Recipient/Sender details.

More information:

[Message Attribute Lookup](#) (see page 304)

<Numericoperator>

For msgattr commands only.

<numericoperator> defines the comparison operator used to test whether the message equals, exceeds or falls below the threshold specified by the <msgvar> and <msgvalue> variables. The operator can be:

<, <=, =, >=, >, <> or numeric

Use these operators if the message attribute being tested has a numeric value, such as the number of recipients or message size. For example, use >= to whether the message size exceeds 25 KB.

WHERE msgsizekb >= 25

Note: Spaces before and after <numericoperator> are optional. For example, tonum>5 and tonum > 5 are equally acceptable.

More information:

[Message Attribute Lookup](#) (see page 304)

<Stringoperator>

For userattr, msgattr, and mapi commands.

<stringoperator> determines whether the specified text, or search term, must be present or absent.

Important! Search terms are defined by the <text> value. You must enclose the <text> search terms in double quotes. This even applies to single-word search terms.

The following operators are supported:

IS or IS ANY

These operators are interchangeable. They define one or more search terms that must be present exactly as specified (although * wildcards are permitted).

The Data Lookup test returns a True value if CA DataMinder detects any of these terms for an individual sender or recipient. (If it detects none of the search terms, the test returns a False value.)

For example, you can use this to detect e-mails, for example, where a recipient is in the Securities Services team:

```
WHERE Team IS "Securities Services"
```

Similarly, you can use this operator to detect emails, for example, where a recipient is in either the London or Paris offices:

```
WHERE Team IS ANY {"London", "Paris"}
```

IS NOT

This operator defines a search term that must not be present. The Data Lookup test returns a True value if CA DataMinder detects this term for an individual sender or recipient. (If this term is not detected, the test returns a False value.)

For example, you can use this to detect e-mails where, for example, none of the recipients are in the Equity Markets team:

```
WHERE Team IS NOT "Equity Markets"
```

IS NOT ALL

This operator defines multiple search terms, none of which must be present. The Data Lookup test returns a True value if CA DataMinder detects none of these terms for an individual sender or recipient. (If any of these terms are detected, the test returns a False value.)

For example, you can use this to detect emails where, for example, none of the recipients are in the Hong Kong, Kuala Lumpur or Tokyo offices:

```
WHERE Office IS NOT ALL {"Hong Kong", "Kuala Lumpur", "Tokyo"}
```

Note: This operator is rarely used in practice.

CONTAINS, CONTAINS ANY, INCLUDES or INCLUDES ANY

These operators are interchangeable. They define one or more search terms that must be present. Implicit leading and trailing * wildcards are added to any search terms specified by this operator. The Data Lookup test returns a True value if CA DataMinder detects any of these terms for an individual sender or recipient. (If none of these terms are detected, the test returns a False value.)

For example, you can use the extract below to detect e-mails where a recipient belongs to a team such as 'Securities Services' or 'Global Securities':

```
WHERE Team CONTAINS "Securities"
```

Similarly, you can use these operators to detect e-mails, for example, where a recipient is in either the Equity Markets, Debt Markets or Securities Services teams:

```
WHERE Team CONTAINS ANY {"Equity","Debt","Securities"}
```

CONTAINS ALL or INCLUDES ALL

These operators are interchangeable. They define multiple search terms that must be present. The Data Lookup test returns a True value if CA DataMinder detects all of these terms for an individual sender or recipient. (If it fails to detect any term, the test returns a False value.)

For example, you can use this to block e-mails where a recipient's team name contains the terms 'Equity' and 'Markets'. The trigger will not activate if the recipient is a member of, for example, the Debt Markets team.

```
WHERE Team CONTAINS ALL {"Equity","Markets"}
```

EXCLUDES or EXCLUDES ALL

These operators are interchangeable. They define one or more search terms that must not be present. The Data Lookup test returns a True value if CA DataMinder detects none of these terms for an individual sender or recipient. (If any of these terms are detected, the test returns a False value.)

This enables you to exempt e-mails if a term is detected (because the test returns a False value so the control trigger will not activate). For example, you can use this to block an email unless one or more recipients is a Manager.

```
WHERE Rank EXCLUDES "Manager"
```

Likewise, you can exempt emails only if a manager or director is included in the recipient list:

```
WHERE Rank EXCLUDES ALL {"Manager","Director"}
```

EXCLUDES ANY

This operator defines multiple search terms that must not be present. The Data Lookup test returns a True value if CA DataMinder fails to detect any of these terms for an individual sender or recipient. (If all of these terms are detected, the test returns a False value.)

This enables you to exempt emails if all of the listed terms are detected (because the test returns a False value so the trigger will not activate). For example, you can use this to block an email unless one or more recipients is a Senior Manager.

```
WHERE Rank EXCLUDES ANY {"Manager", "Senior"}
```

Note: When using the CONTAINS or EXCLUDES operators, be aware that it is often more efficient to use the IS or IS NOT operators, respectively. The example below uses an exact match:

```
msgattr WHERE %recipient% IS "Sales"
```

and is therefore more efficient than the following example, which infers a substring match:

```
msgattr WHERE %recipient% CONTAINS "Sales"
```

More information:

[Address Book Lookup](#) (see page 301)

[Message Attribute Lookup](#) (see page 304)

[User Attribute Lookup](#) (see page 297)

<Text>

For userattr and mapi commands only.

<text> represents the search term (or terms) whose presence or absence you want to test. For example, if <uservar> is set to Department, you may want to set <text> to Sales or Marketing.

Important! Double quotes: You must enclose search terms in "double quotes"! This even applies to single-word search terms. For example:

```
{"Equity", "Debt", "Securities"}
```

Case-insensitive

Search terms are not case sensitive. For example, if <uservar> and <text> jointly specify the Sales department, then Sales, sales and SALES all return a True value if detected.

MemberOf

The MemberOf variable (see <uservar>) looks for the mail group or distribution list Display name.

Multiple search terms: If required, you can specify a list of multiple search terms as the <text>. For example, you can define multiple search terms if <operator> is set to CONTAINS ANY or EXCLUDES ANY. The format for multiple terms is shown in the example below:

```
{"Manager", "Director", "Reviewer"}
```

Note that search term lists are comma-separated and enclosed in curly brackets: { }

Wildcards

If required, you can use ? and * wildcards when defining search terms. For example, 'ma*' would match both Marketing and Management.

More information:

[Address Book Lookup](#) (see page 301)

[User Attribute Lookup](#) (see page 297)

[Enable Regionalized Policy Engine Lookup](#) (see page 299)

<Type>

For userattr, mapi and msgattr commands.

<type> determines the type of Data Lookup command. The different types of command have slight differences in syntax and accept different variables. The following types are supported:

userattr

This defines a User Attribute lookup command. The basic command syntax is:

```
userattr WITH <who> WHERE <uservar> <operator> <text>
```

mapi

This defines an Address Book lookup command. The basic command syntax is:

```
mapi WITH <who> WHERE <uservar> <operator> <text>
```

msgattr

This defines a Message Attribute lookup command. The basic command syntax is:

```
msgattr WHERE <msgvar> <msgoperator> <msgvalue>
```

xmlattr

This defines an XML Attribute lookup command. The basic command syntax is:

```
xmlattr WITH <xpath> WHERE <xpath> <stringoperator|numericoperator>  
<attribvalue>
```

More information:

[Address Book Lookup](#) (see page 301)

[Message Attribute Lookup](#) (see page 304)

[User Attribute Lookup](#) (see page 297)

<Uservar>

For userattr and mapi commands only.

<uservar> is a CA DataMinder user attribute or group or an Outlook Address Book property. It is this attribute, group or property that is tested for a True or False match against the Data Lookup criteria.

CA DataMinder user attribute

(User Attribute lookup only) These are the customized user attributes defined for your CA DataMinder installation. Specify the name of the user attribute that you want to test against.

For example, if a 'Team Name' attribute has been created for your organization, you can specify this as the <uservar> by typing

```
WHERE "Team Name" IS "Sales"
```

Note: User attributes are not case sensitive. Always enclose the attribute name in double quotes, for example, "Rank" or "Team Name".

CA DataMinder user group

(User Attribute lookup only) You can configure lookup commands to test which CA DataMinder user group a user belongs to. In effect, data lookup handles the user's parent group as if it were a user attribute.

Wgn.Group

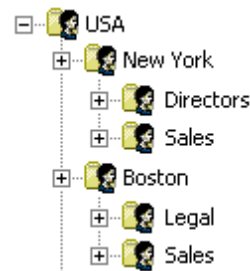
Use this variable to specify a specific parent user group that you want to test against. For example, to configure a trigger to block emails sent to members of the Sales user group, the command syntax is:

```
WHERE Wgn.Group IS "Sales"
```

If multiple groups exist with the same name in different branches of the user hierarchy, Data Lookup tests all matching groups.

Wgn.GroupParent

Use this variable to specify a user group that heads a specific branch of the user hierarchy. Data Lookup tests whether the user belongs to a user group within this branch. For example, consider this user hierarchy:



To configure a trigger to block emails sent to members of the Boston Legal or Boston Sales groups, the command syntax is:

```
WHERE Wgn.GroupParent IS "Boston"
```

Note: Be aware of the following:

- Both Wgn.Group and Wgn.GroupParent also support the CONTAINS operator. For example:
WHERE Wgn.Group CONTAINS {"Sales","Legal"}
- Group names are not case sensitive. Always enclose the group name in double quotes, for example, "Legal" or "New York".

Address Book special property

(Address Book lookup only). These properties are:

- Title
- Department
- Office
- City

- State
- Country
- Region

Note: Country and Region refer to the same Address Book property

- MemberOf

Refers to membership of a mail group or distribution list. MemberOf takes the group or list Display Name as its <keytext> match.

Note: MemberOf cannot check [nested groups or lists](#) (see page 336).

Note: You cannot use MemberOf in lookups commands that query Lotus Domino directories.

Address Book extension attribute

(Address Book lookup only) Extension attributes are custom user attributes created in Active Directory and used by Address Books in Outlook. Administrators can define up to 15 custom attributes per user. For example:

ExtensionAttribute3

This refers to Custom Attribute 3, as defined in the advanced Exchange user properties in Active Directory. (In the examples, Custom Attribute 3 identifies an employee's hire date.)

Note: For details about custom user attributes, see your Active Directory documentation.

Address Book hexadecimal property code

(Address Book lookup only) Code numbers identify Address Book properties in the Active Directory schema. The correct <var> syntax is:

MAPIID0x<n>

Where <n> is the hexadecimal code.

Note: You may need to calculate hexadecimal codes from the decimal schema codes. For details about the schema, see your Active Directory documentation.

mandatory <uservar>

The mandatory keyword ensures that control triggers always activate when required, or equally important, do not activate unnecessarily. The example below specifies that the lookup command must detect a value for the 'Team' attribute, otherwise the entire command will fail to run:

WHERE mandatory Team IS "Equity Debt"

ObjectCategory <person, group, or dynamicgroup>

(Address Book lookup only) ObjectCategory tests the recipient category. It allows you to write lookup commands that can detect recipients who are actual people, not distribution groups.

ObjectCategory supports the following recipient categories:

person

Identifies mailbox users, contacts, shared mailboxes, and special Exchange mailboxes (such as an Equipment mailbox or Room mailbox). In effect, 'person' identifies any recipient that is *not* a distribution group or dynamic distribution group.

group

Identifies distribution groups (also called distribution lists or DLs).

dynamicgroup

Identifies dynamic distribution groups.

Example

For example, you can use ObjectCategory to set up an email trigger to enforce information boundaries. In the following example, the trigger fires if a user sends an email to a person outside of the Finance department. The trigger also fires if the email is sent to a distribution group that includes members who are not in the Finance department.

MAPI with ANY %recipient% where (objectCategory is not "group") and (department is not "finance")

Without the ObjectCategory test, the lookup may return 'True' if the recipient is a distribution group (because distribution groups may not have a Department property). In turn, this could cause the trigger to fire and possibly block the email from being sent to legitimate recipients.

More information:

[Address Book Lookup](#) (see page 301)

[User Attribute Lookup](#) (see page 297)

MemberOf Data Lookup does not Check Nested Groups or Lists

Important! If you use the MemberOf variable to detect outgoing e-mails, be aware that MemberOf does not check for membership of nested mail groups or distribution lists.

For example, an organization has an 'All US' distribution list. This list contains several nested lists, including 'All Chicago'. If MemberOf is set to detect members of the 'All US' mail group, the trigger will not activate when sent to members of 'All Chicago' unless these users are also explicitly members of 'All US'.

Note: You cannot use MemberOf in lookup commands that query Lotus Domino directories.

Mandatory Keyword - Data Lookup Commands

The mandatory keyword ensures that email triggers always activate when required, or equally important, do not activate unnecessarily.

Normally, <uservar> specifies an Outlook Address Book property or a CA DataMinder user attribute, the presence or absence of which determines whether the lookup command returns a True value. But if no value has been set for the attribute or property (for example, the CA DataMinder account for a new recruit has not been updated to show their Team), or the specified address book property does not exist (for example, the lookup command specifies 'Titel' instead of 'Title'), CA DataMinder ignores this omission and evaluates the remaining True-False tests within the data lookup command. In the worst case, this could mean that a trigger fails to activate, allowing an email to be sent to a proscribed recipient.

For example, you have configured a lookup command to block emails sent between the Research and Investment Banking (IB) teams. But a new member of the IB team has not been added to the IB mail group (that is, their MemberOf address book property is not up to date). Consequently, when a researcher sends an email to this new IB member, the lookup command fails to identify him or her as a proscribed recipient, so the control trigger does not activate and the email is not blocked.

To eliminate these risks, you can qualify <uservar> with the mandatory keyword. The example below specifies that the lookup command must detect a value for the 'Team' attribute, otherwise the entire command will fail to run:

```
WHERE mandatory Team IS "Equity Debt"
```

Using the mandatory keyword ensures that if no value has been set for the specified attribute or property, or if the address book property does not exist, the data lookup command always returns an error, so invoking the Data Lookup Failure Mode setting.

Note: For userattr commands, if the specified attribute does not exist (for example, the lookup command specifies 'Teem' instead of 'Team'), the data lookup command always returns an error, regardless of whether mandatory is used or not, so invoking the Data Lookup Failure Mode setting.

<Xpath>

For xmlattr commands only.

<xpath> specifies the location of an element (or node) within an XML hierarchy. Specifically, xmlattr lookup commands use <xpath> to locate the emails or file attribute, stored as an XML element, whose value they need to test (where this value is specified by <attribvalue>).

Email example

The example below specifies an email x-header named 'x-vpm-state'. The x-header name is stored as a property set.

```
xmlattr WHERE apm/event/email/header/item[@name='x-vpm-state']
```

File examples

The examples below specify, respectively, a file event's file name, file size, the date when the file was last modified, and a property set named 'ID'.

```
xmlattr WHERE apm/event/file/filename
xmlattr WHERE apm/event/file/size
xmlattr WHERE apm/event/file/modified
xmlattr WHERE apm/event/file/property_set[@name="ID"]
```

Properties in a property set

<xpath> can also specify the location within an XML hierarchy of a property set or an individual property within a property set. For emails, x-header names are stored as property sets. For files, property sets are effectively collections of related file attributes.

In this situation, <xpath> actually specifies the name attribute of a 'property set' or 'property' element. For example, Microsoft Word documents can include a 'Custom' property spot. This can include any custom properties defined for that document, such as 'Security' and 'Status'. The example below locates the Custom property set:

```
xmlattr WHERE apm/event/file/property_set[@name="Custom"]
```

<xpath> can also specify an individual property within a property set. The example below locates the Security property within the Custom property set:

```
xmlattr WHERE apm/event/file/property_set[@name="Custom"]/property[@name="Security"]
```

In all cases, the @name property identifier must be enclosed in square brackets. Two example property sets are included in the XML metadata.

More information:

[XML Attribute Lookup Examples](#) (see page 309)

[XML Metadata for Word Documents](#) (see page 311)

[XML Attribute Lookup](#) (see page 306)

Complex Data Lookup Commands

For precision targeting of specific emails, you can use AND, OR and NOT operators and parenthesis to define more complex Data Lookup commands. These enable you to include multiple True-False tests within a single command or link separate commands. But first note the rules governing command evaluation.

Command Evaluation

CA DataMinder evaluates lookup commands from left to right. This is particularly important if your lookup command contains three or more True-False tests and if you use brackets to set evaluation precedence. Note that we do generally recommend you use brackets when combining multiple lookup commands. The examples below show how three logical tests (A, B and C) combine to produce an overall result:

Example tests		Results
1	A AND B AND C	False
2	A OR B OR C	True
3	A OR B AND C	True
4	A AND B OR C	True
5	B AND (A OR C)	False
Where A and C are True, and B is False.		

When you combine multiple lookup commands, CA DataMinder quits evaluating as soon as it detects any subcommand that allows the overall command to be unambiguously resolved. Specifically, this affects:

- Any instances where the first subcommand returns False (because this sets the overall command to False, so the trigger does not activate).
- Subcommands linked with an OR operator. Here, CA DataMinder quits evaluating if any subcommand returns True (because this sets the entire command to True and activates the trigger).

In examples 2 and 3 above, if A, B and C represent linked commands, then commands B and C are not evaluated because, with command A returning True, the overall command must also return True. This is a deliberate optimization designed to minimize delays when processing outgoing emails.

Note: This optimization does not apply to multiple True-False tests within a single lookup command. In this case, all tests are fully evaluated.

Simple True-False Tests

Simple True-False test: positive operator, IS

This example is a simple True-False test that uses the positive operator IS, in the following single lookup command:

```
mapi with %recipient% where dept IS "sales"
```

When %recipient% is used with IS in this way, the operator ANY is implicit, so the lookup command is actually as follows:

```
mapi with ANY %recipient% where dept IS "sales"
```

If there are three recipients, this command requires the following three lookup operations:

```
(mapi with srimmel@unipraxis.com where dept IS "sales") OR  
(mapi with lsteel@unipraxis.com where dept IS "sales") OR  
(mapi with fschaeffer@unipraxis.com where dept IS "sales")
```

For the test to be true, only one of the lookup commands needs to be true. That is, if Spencer is in the Sales department, the lookup command is true and does not check to see if Lynda and Frank are also in the Sales department.

If you want to use ALL with the same lookup command, you need to add it explicitly, as shown below:

```
mapi with ALL %recipient% where dept IS "sales"
```

With the same three recipients, this command requires the following three lookup operations:

```
(mapi with srimmel@unipraxis.com where dept IS "sales") AND (mapi with lsteel@unipraxis.com where dept IS "sales") AND (mapi with fschaeffer@unipraxis.com where dept IS "sales")
```

This time, for the test to be true, all three lookup commands must be true. That is, Spencer, Lynda and Frank must all be in the Sales department for the test to be true.

Simple True-False test: negative operator, IS NOT

This example is a simple True-False test that uses the negative operator IS NOT, in the following single lookup command.

```
mapi with %recipient% where dept IS NOT "sales"
```

When %recipient% is used with IS NOT in this way, the operator ALL is implicit, so the lookup command is actually as follows:

```
mapi with ALL %recipient% where dept IS NOT "sales"
```

If there are three recipients, this command requires the following three lookup operations:

```
(mapi with srimmel@unipraxis.com where dept IS NOT "sales") AND (mapi with lsteel@unipraxis.com where dept IS NOT "sales") AND (mapi with fschaeffer@unipraxis.com where dept IS NOT "sales")
```

For the test to be true, all three lookup commands must be true. That is, Spencer, Lynda and Frank must all be in a department other than 'Sales' for the test to be true.

If you want to use ANY with the same lookup command, you need to add it explicitly, as shown below:

```
mapi with ANY %recipient% where dept IS NOT "sales"
```

With the same three recipients, this command requires the following three lookup operations:

```
(mapi with srimmel@unipraxis.com where dept IS NOT "sales") OR (mapi with lsteel@unipraxis.com where dept IS NOT "sales") OR (mapi with fschaeffer@unipraxis.com where dept IS NOT "sales")
```

For the test to be true, only one of the lookup commands needs to be true. That is, if Spencer is not in the Sales department, then that lookup command is true and the details for Lynda and Frank are not checked.

More information:

[Address Book Lookup](#) (see page 301)

Complex True-False Test

The next example is a complex True-False test. It uses the positive operator IS in both lookup sub-tests within the following single lookup command:

```
mapi with %recipient% where (dept IS "sales") AND (position IS "manager")
```

If there are three recipients, this command requires the following three lookup operations, each containing two lookup sub-tests.

```
(mapi with srimmel@unipraxis.com where (dept IS "sales") AND (position IS "manager") ) OR  
(mapi with lsteel@unipraxis.com where (dept IS "sales") AND (position IS "manager") ) OR  
(mapi with fschaeffer@unipraxis.com where (dept IS "sales") AND (position IS "manager") )
```

For such a lookup command to be True, both subtests must be true. For example, for the first lookup command to be true, Spencer must be a manager and in the Sales department.

For the test itself to be true, only one of the three lookup operations needs to be true. That is, if Spencer is a manager and in the Sales department, then the test is true and the details for Lynda and Frank are not checked.

More information:

[Message Attribute Lookup](#) (see page 304)

Composite True-False Test

You can combine multiple commands using AND, OR and NOT operators. For example, you can combine multiple msgattr commands to detect messages that exceed a maximum size or where the number of recipients exceeded a maximum limit. You can even link totally disparate commands. This is particularly useful if you want to combine different types of Data Lookup command. All in cases, the syntax is:

```
[NOT] (CMD1) AND|OR [NOT] (CMD2) [AND|OR [NOT] (CMD3)]
```

Where (CMDn) is a complete, self-contained userattr, mapi or msgattr data lookup command.

For example, you can combine Message Attribute and Address Book lookup commands to block e-mails sent to the La Paz or Lima offices unless the total message impact is less than 5MB. The syntax is:

```
NOT (msgattr WHERE msgimpactkb < 5000)
AND (mapi WITH any %recipient% WHERE Office CONTAINS ANY {"La Paz","Lima"})
```

The following is another example of a composite True-False test. It uses the positive operator IS with two sub-commands.

```
(mapi with %sender% where dept IS "sales") AND (userattr with %recipient% where position IS "manager")
```

If there is one sender and three recipients, this command requires the following three lookup operations, each containing two sub-operations:

```
((mapi with oabassi@unipraxis.com where dept IS "sales") AND
(userattr with srimmel@unipraxis.com where position IS "manager"))
OR
((mapi with oabassi@unipraxis.com where dept IS "sales") AND
(userattr with lsteel@unipraxis.com where position IS "manager"))
OR
((mapi with oabassi@unipraxis.com where dept IS "sales") AND
(userattr with fschaeffer@unipraxis.com where position IS "manager"))
```

For any lookup operation to be true, both its sub-operations must be true. For example, for the first lookup operation to be true, Omar must be in the Sales department and Spencer must be a manager.

For the test itself to be true, only one of the three lookup operations needs to be true.

More information:

[Address Book Lookup](#) (see page 301)

[Message Attribute Lookup](#) (see page 304)

Complex Composite True-False Test

The following example is a complex composite True-False test. It contains two sub-lookups, one of which contains two sub-tests.

```
(mapi with %sender% where dept IS "sales") AND
(mapi with %recipient% where (dept IS "marketing") AND (position IS "manager"))
```

If there is one sender and three recipients, then this command requires the following four lookup operations, three of which contain two sub-tests.

```
(  
  mapi with oabassi@unipraxis.com where dept IS "sales") AND  
  ((mapi with srimmel@unipraxis.com where (dept IS "sales")  
    AND (position IS "manager"))  
    OR  
    (mapi with lsteel@unipraxis.com where (dept IS "sales")  
      AND (position IS "manager"))  
    OR  
    (mapi with fschaeffer@unipraxis.com where (dept IS "sales")  
      AND (position IS "manager"))  
)
```

For an operation to be true, all of its sub-operations must be true.

For the test itself to be true, the first simple lookup operation and at least one of the three other operations need to be true.

More information:

[Address Book Lookup](#) (see page 301)

OR and <fallguy> Handling

If you combine multiple lookup commands, CA DataMinder quits evaluating as soon as a subcommand returns a True or False value that allows the overall command to be unambiguously resolved. This is a deliberate optimization designed to minimize delays when processing outgoing emails.

But for commands linked with an OR operator, it could mean, in certain circumstances, that the <fallguy> variable only returns recipients identified by one subcommand (because, with a True value already returned, there is no logical need to evaluate the other subcommands).

For example, a combined lookup command detects emails sent to the London office (subcommand A) OR members of the Sales team (subcommand B). It evaluates subcommand A first. If it successfully detects a London recipient, the overall command must also be True so there is no logical need to evaluate subcommand B. This means that no Sales recipients are written to the <fallguy> variable. If this variable is included in a notification dialog, shown when the control trigger activates, the message to users may contain an incomplete list of 'triggering' recipients.

Counting Unique Domains

An important feature of Message Attribute (msgattr) lookup is the ability to count the number of unique domains in a list of e-mail recipients. This enables administrators to block users from sending individual e-mails to, for example, more than five companies at a time.

This feature relies on CA DataMinder successfully extracting the domain element of an SMTP e-mail address. The domain element comprises either two segments ('short domain') or three segments ('long domain') after the '@' symbol. For example:

- **Short domain:** spencerrimmel@unipraxis.com
- **Long domain:** spencerrimmel@unipraxis.co.uk

When extracting the domain from an SMTP e-mail address, CA DataMinder always assumes this is a short domain and so extracts the final address two segments unless these final two segments match any one of a list of known exceptions, in which case CA DataMinder infers that it must extract a long domain (that is, the final three segments).

Long domain example

Consider an e-mail sent to two recipients, lsteel@unipraxis.co.uk and srimmel@monitrax.co.uk.

It is clear from the recipient addresses that the e-mail is being sent to two companies, Unipraxis and Monitrax. But if CA DataMinder did not have the ability to extract long domains, it would only extract the final two address segments, 'co.uk', and so would incorrectly infer that the domain was the same for both recipients (giving a unique domain count of 1).

However, because '*.uk' is one of the known domain exceptions, when CA DataMinder detects '.co.uk' in an e-mail address it recognizes this as part of a long domain and so extracts the final three segments. In the example above, this enables CA DataMinder to recognize that the two recipients belong to two different companies and so it correctly calculates the unique domain count to be 2.

List of known long domains

This list of known exceptions is hard-coded within CA DataMinder and includes all commonly used long domain patterns such as '*.uk' and '.ru.com'. However, as the list of worldwide domains continues to grow, it is inevitable that new long domains will emerge that do not match this hard-coded list.

If required, you can also supplement this list in the user policy; to do this, edit the Additional Long Domain Endings setting.

Adding to the list of long domains

If you do need to supplement the default list of long domain patterns, you need to edit the Additional Long Domain Endings user policy setting; find this in the Definitions policy folder. When you edit this setting, be aware of the following:

- All entries must start with a period and contain exactly two periods, for example:
.ins.kr .fin.tz
- If required, you can use a * wild card in place of an entire segment, for example:
.*.pb

However, we recommend you avoid using wildcards where possible because the scope of the resulting match may be greater than anticipated, causing in short domains to be inadvertently treated as long domains. This is particularly true if the domain element of an address includes a geographical subdomain. For example, adding '.*.pb' to the exceptions list would cause CA DataMinder to treat ny.unipraxis.pb and london.unipraxis.pb as separate domains.

Default List of Long Domains

CA DataMinder uses the email address patterns listed below to identify 'long domains' when extracting the domain element from an SMTP address. Long domains are defined as comprising three segments after the @ symbol, for example, lsteel@unipraxis.co.uk. You can also supplement this list in the user policy; to do this, edit the Additional Long Domain Endings setting in the Definitions folder.

Note: The ability to identify long domains is required by msgattr lookup commands when counting the number of unique domains in a list of email recipients.

.*.au	.bj.cn	.fm.br	.he.cn	.mi.th	.odo.br	.ru.com
.*.hk	.br.com	.fot.br	.hi.cn	.mil.*	.on.ca	.sa.com
.*.nz	.cn.com	.fst.br	.hk.cn	.mo.cn	.or.ac	.sc.cn
.*.uk	.cng.br	.g12.br	.hl.cn	.muni.il	.or.at	.school.za
.ab.ca	.cnt.br	.gb.com	.hn.cn	.nb.ca	.or.jp	.sd.cn
.ac.*	.co.*	.gb.net	.hu.com	.ne.jp	.or.kr	.se.com

.ad.jp	.com.*	.gd.cn	.ind.br	.ne.kr	.or.th	.sh.cn
.adm.br	.cq.cn	.geo.jp	.inf.br	.net.*	.org.*	.sk.ca
.adv.br	.de.com	.go.jp	.info.ro	.nf.ca	.pe.ca	.slg.br
.ah.cn	.ecn.br	.go.kr	.jl.cn	.ngo.za	.ppg.br	.sn.cn
.alt.za	.ed.jp	.go.th	.jor.br	.nm.cn	.presse.fr	.store.ro
.am.br	.edu.*	.gov.*	.js.cn	.nm.kr	.pro.br	.sx.cn

.arq.br	.eng.br	.gov.*	.jx.cn	.no.com	.psc.br	.tj.cn
.art.br	.ernet.in	.gr.jp	.k12.il	.nom.br	.psi.br	.tm.fr
.arts.ro	.esp.br	.gs.cn	.k12.tr	.nom.ro	.qc.ca	.tm.mc
.asso.fr	.etc.br	.gv.ac	.lel.br	.nom.za	.qc.com	
.asso.mc	.eti.br	.gv.at	.lg.jp	.ns.ca	.qh.cn	
.au.com	.eu.com	.gx.cn	.ln.cn	.nt.ca	.re.kr	

.bbs.tr	.fin.ec	.gz.cn	.mb.ca	.nt.ro	.rec.br	
.bc.ca	.firm.ro	.ha.cn	.med.br	.ntr.br	.rec.ro	
.bio.br	.fj.cn	.hb.cn	.med.ec	.nx.cn	.res.in	

Chapter 24: User Notifications

The Intervention setting in a control action enables you to block, warn or inform user, and to display a notification dialog, or send a notification email, containing an explanatory message.

In addition, Data At Rest actions enable you to replace a user's file with a file of the same name containing a message to the user and email control actions enable you to forward emails to another address, with the forwarded email included as an attachment or thread within a notification email.

In all cases, you can configure the text displayed to the user. Specifically, you can define the title and message in the notification dialog, and the subject and body text in the notification email, or the text of the replacement file. You can also use variables to customize the text content so it reflects the condition that caused the control trigger to activate.

This section contains the following topics:

[Notification Dialogs](#) (see page 347)

[Notification Emails - Containing Forwarded Emails](#) (see page 350)

[Replacement Files](#) (see page 350)

[Variables in User Notifications and Email Replies](#) (see page 351)

[Variables in User Notifications for File Events](#) (see page 357)

Notification Dialogs

For each control trigger, you can define a message that appears in the notification dialog when the trigger activates. You can use variables to customize the text content so it reflects the condition that caused the control trigger to activate. You can also use delimiters to tag sections of the message as selectable, enabling users, for example, to copy missing disclaimers directly from the notification dialog into an e-mail or attachment.

Some control triggers even allow you to define multiple messages, so that the message seen by users varies according to the key text detected by the trigger. Finally, you can configure the titles of the various notification dialogs.

Notification Dialog Titles

You can configure the title that appears in the various CA DataMinder advisory dialogs. For example, you can define dialog titles for blockings and warnings.

Find the relevant settings in the System Settings, User Notifications folder of the user policy.

Notification Dialog Messages

You can customize the message that appears in the notification dialogs triggered by the Intervention setting. You can enter a different message for each control trigger. For example:

Trigger	Example message to user
URL n	This URL site is prohibited. You are not authorized to view this Web page.
File Upload n	Corporate guidelines do not permit you to upload files to this Web site.
Document Classifier n	Corporate guidelines do not permit you to send sales proposals unless they contain an official disclaimer.
Attachments n	You are not authorized to open this email. It contains an attachment that includes inappropriate material.

Multiple message control triggers

Some triggers allow you to define separate messages for each item in a list of key words or phrases. When CA DataMinder detects that word or phrase, it displays the corresponding message. This allows you to tailor the message to give the user as much detail as possible, using a single control trigger. To configure multiple messages, you edit a list setting in the relevant control trigger.

More information:

[Multiple Message List Items](#) (see page 71)

Copying Text from Notification Messages

When defining notification messages, you can configure them so that users can copy selected phrases directly from the advisory dialog into other documents. This is most useful when an outgoing email or attachment lacks an official disclaimer. You can configure a control trigger to display a warning message that includes the missing disclaimer. The user can then copy the disclaimer directly into the email or attachment before resending it.

To set notification messages with selectable text that users can copy

1. In the user policy, expand the control trigger you want and select the Message To Users setting.
2. Double-click this setting or right-click and choose Properties.
3. In the Policy Setting Properties dialog, enter the notification message.

To tag words or phrases as selectable, add two __ characters (underscores) as delimiters before and after the relevant section of the message.

4. Make sure the control trigger is associated with a control action that displays a notification message.

That is, make sure the Intervention setting in the control action is set to 'Block with notification', 'Warn', or 'Inform'.

5. Save the policy changes.

When the control trigger activates, the resulting notification dialog contains a message with the tagged, selectable section shown in bold.

The user can now copy the text from the notification dialog directly into the original email or another document (such as an attachment). The user can either drag and drop the message text directly, or they can copy and paste it.

Drag and drop the notification message

As soon as the user drags the message text, this cancels the notification dialog. (Drag and drop is not supported for emails in Lotus Notes.)

Copy and paste the notification message

1. First, the user must right-click the bold text and choose Copy.
2. Next, they must click OK or Cancel to clear the notification dialog.

Important! For Inform and Warning dialogs, if the user clicks Continue, the email is sent immediately, before the user can paste in the missing text!

3. Finally, the user can paste the text into their email or attachment before resending the email.

Notification Emails - Containing Forwarded Emails

You can define the text content of notification emails. These are emails containing emails that have been intercepted and forwarded by a control trigger. You can define separate text for 'incoming email' and 'outgoing email' notification emails.

Subject and body text

For each user policy, you can define the subject and body text in a single 'incoming' notification email and a single 'outgoing' notification e-mail. You can also use variables to customize the e-mail subject and body text, for example, to refer to the original sender's email address.

Unlike the messages in notification dialogs, you cannot specify separate notification emails for each control trigger or control action. Instead, to define the subject and body text you must edit the relevant system settings in the user policy. You can find these settings in the System Settings, User Notifications, Forwarded E-mail Settings policy folder.

Examples

Forwarded email	Example email subject
Incoming	Incoming -mail for %To% requires your attention
Outgoing	Please authorize the attached outgoing email
Forwarded email	Example email body text
Incoming	The email "%Subject%" may breach corporate guidelines. It has been forwarded to you for authorization.
Outgoing	Review the attached email sent by %From%. If the email adheres to corporate guidelines, please forward it to the intended recipient, %To%.
Incoming or outgoing	%default%

Replacement Files

For each Data At Rest control trigger, you can define a message to appear in a replacement file when the trigger activates. You can use variables to customize the text content so it reflects the condition that caused the control trigger to activate.

Variables in User Notifications and Email Replies

When defining the text in a notification dialog, notification email, automatic email reply, or replacement file message to users, you can use variables to represent certain types of information and to customize the text content based on the circumstances of the control event. For example, if a control trigger displays a warning when users browse to various Web sites, you can use the %URL% variable to include the actual URL in your notification message.

Note:

- Variables are not case-sensitive. So, for example, you can type %URL% or %url% when defining a notification message.
- The exact format of the email address replacement string depends on the type of email address. For SMTP mail it is for example "Spencer Rimmel(spencerrimmel@unipraxis.com)" and for Exchange mail "Spencer Rimmel(spencer rimmel(unipraxis))". This applies to the %address%, %to%, %from%, %cc%, and %bcc% variables.

The supported variables follow:

%Address%

Displays the email address, or addresses, that caused the control trigger to activate. For outgoing emails, this is the recipient addresses; for incoming emails, it is the sender address.

For example, these messages in the policy:

You are not authorized to send emails to %Address%.

You are not authorized to receive emails from %Address%.

Display like this in notification messages:

You are not authorized to send emails to Spencer

Rimmel(spencerrimmel@unipraxis.com), Frank

Scheffer(frankscheffer@unipraxis.com).

You are not authorized to receive emails from Spencer

Rimmel(spencerrimmel@unipraxis.com).

%Application%

Displays the application that activated an Application Monitor control trigger

For example, this message in the policy:

You are not authorized to run %Application%.

Displays like this in a notification message:

You are not authorized to run Netscape.

%ApplicationPath%

Displays the path and executable name of the application that activated an Application Monitor control trigger. For example, this message in the policy:
CA DataMinder has detected %ApplicationPath% starting up.

Displays like this in a notification message:
CA DataMinder has detected c:\program files\netscape\netscp.exe starting up.

%BCC%

Displays any recipients listed in the Bcc: field of a forwarded email.

For example, if the user policy specifies this message for the body text of the notification email:

The attached email has been forwarded to you for approval because the Bcc: addressees include %BCC%.

It displays like this in a notification email:

The attached email has been forwarded to you for approval because the Bcc: addressees include Spencer Rimmel(spencerrimmel@unipraxis.com).

%CC%

Displays any recipients listed in the Cc: field of a forwarded email.

For example, this message in the policy:

You are not authorized to use credit card number %CCN%.

Displays like this in a notification message:

You are not authorized to use credit card number 4100 1234 1234 1234.

Note: The display of credit card numbers in notification messages is subject to the same constraints as elsewhere in CA DataMinder. This is governed by the Sensitive Information Handling setting in the System Settings folder.

%CCN%

Displays the credit card number detected by CA DataMinder and which activated a Credit Card control trigger.

For example, this message in the policy:

You are not authorized to use credit card number %CCN%.

Displays like this in a notification message:

You are not authorized to use credit card number 4100 1234 1234 1234.

Note: The display of credit card numbers in notification messages is subject to the same constraints as elsewhere in CA DataMinder. This is governed by the Sensitive Information Handling setting in the System Settings folder.

%Default%

(For the body text of notification emails and automatic email replies only.)

Displays summary details about the forwarded email. For example, this body text in the policy:

%default%

Displays details like this in the notification email:

The original mail message is:

From: lyndasteel@unipraxis.com

To: Spencer Rimmel <EX:/O=UNIPRAXIS/OU=UK/CN=RIMMEL/CN=SPENCER>

Subject: Corporate Restructing

%From%

Displays the original sender of an email that was detected by a control trigger and forwarded to another address.

For example, if the user policy specifies this message for the body text of a notification email:

An email from %FROM% has been intercepted and forwarded to you for approval.

It displays like this in a notification email:

An email from Lynda Steel(lyndasteel@unipraxis.com) has been intercepted and forwarded to you for approval.

%Keysting%, %Keyword%

Display the word or phrase detected by CA DataMinder in a Web page, email or file and which caused a control trigger to activate.

For example, this message in the policy:

Warning: This email refers to %Keysting%. Such references are normally prohibited in corporate correspondence.

Displays like this in the notification message:

Warning: This email refers to Project Alpha. Such references are normally prohibited in corporate correspondence.

Note: In practice, these variables are interchangeable but you may find notification messages easier to maintain if you use the variables in their 'natural' context. That is, you use %Keyword% to represent single words and %Keysting% for phrases or sentences.

%Keystrength%

Displays the keystrength of the encryption algorithm used on a Web site.

For example, this message in the policy:

This site uses %Keystrength% encryption. You are only permitted to browse sites that use at least 256 bit encryption.

Displays like this in a notification message:

This site uses 128 bit encryption. You are only permitted to browse sites that use at least 256 bit encryption.

Note: %Keystrength% does not return a value when used in a URL control trigger (because the trigger activates as soon as it detects the URL, before CA DataMinder can check the encryption level). Also, be aware of the browser requirements when exempting secure Web sites.

%MailDateTime%

Displays the time and date when an incoming email was received and when outgoing email was sent.

For example, if the user policy specifies this message for the Subject of the notification email:

Unauthorized email detected: %MailDateTime%

It displays like this in the notification email:

Unauthorized email detected: 16/05/2003 8:23

You cannot configure the date and time format from within CA DataMinder. The format shown in a notification email is determined by the short date format defined for the local machine.

%MessageClass%

Displays the message class of a captured email, such as IPM.Schedule.Meeting.Request.

This variable is primarily for testing purposes. Using msgattr lookup commands, you can exclude specific types of email such as read receipts and meeting requests. The %MessageClass% variable lets you confirm that the correct message classes are being detected.

%MessageToUsers%

Displays the value of the Message To Users setting.

For example, you can forward blocked emails to a manager. You can also specify separate notification messages for the original sender and the manager. If the user policy specifies:

- This message for the 'Trigger/Message to Users' setting in the trigger:
References to %Keystring% are prohibited in corporate correspondence.
- This message for the 'System Settings/User Notifications/Forwarded E-mail Settings/Outgoing Body' setting:
The attached mail was blocked. The message displayed to the sender was "%MessageToUsers%".

Then, the forwarded email contains this message:

The attached mail was blocked. The message displayed to the sender was "References to Project Alpha are prohibited in corporate correspondence."

%Site%

Displays the 'site' element of a Web site URL or the 'organization' element of an email address. This can be useful if you want to make the notification message easier to read.

For example, these messages in the policy:

You are not authorized to browse the %Site% Web site.

You are not authorized to send emails to %Site%.

Display like this in notification messages:

You are not authorized to browse the Unipraxis Web site.

You are not authorized to send emails to Unipraxis.

%SSN%

Displays the social security number detected by CA DataMinder and which activated a classifier, keystring or attachment trigger.

For example, this message in the policy:

An email containing the social security number %SSN% has been intercepted for review. You are not authorized to send personally identifiable information.

Displays like this in a notification message:

An email containing the social security number 123-45-6789 has been intercepted for review. You are not authorized to send personally identifiable information.

CA DataMinder uses a sophisticated recognition process to cross-check against an imported list of currently available SSNs. That is, the US Social Security High Group File. To ensure that this data is accurate, we recommend you update this text file on a regular basis (for example, monthly).

%Subject%

Displays the Subject of the forwarded email.

For example, if the user policy specifies this message for the body text of the notification email:

The email "%Subject%" has been intercepted and forwarded to you for approval.

It displays like this in the notification email:

The email "Corporate Restructuring" has been intercepted and forwarded to you for approval.

Note the optional use of double-quotes to highlight the Subject reference in the notification email.

%To%

Displays any recipients listed in the To: field of a forwarded email.

For example, if the user policy specifies this message for the body text of the notification email:

The attached email has been forwarded to you for approval because it was addressed to %To%.

It displays like this in a notification email:

The attached email has been forwarded to you for approval because it was addressed to Spencer Rimmel(spencerrimmel@unipraxis.com).

%TriggerName%

Displays the value of the Trigger Name setting.

For example, if the user policy specifies this message for the 'Trigger/Message to Users' setting in the trigger:

This message or the associated attachment(s) you are attempting to send is in possible violation of a corporate intellectual property rights policy called "%triggername%".

Then it displays like this in a notification email:

This message or the associated attachment(s) you are attempting to send is in possible violation of a corporate intellectual property rights policy called "Patent Applications".

%URL%

Displays the URL of the Web site that activated the trigger.

For example, this message in the policy:

You are not authorized to browse %URL%.

Displays like this in a notification message:

You are not authorized to browse `http://www.unipraxis.com`.

Note: Any query strings are excluded from the URL displayed in the message. This is the part of a URL containing the search parameters when submitting data to a dynamic Web site. For example, `id=LogiCard` is a query string in this URL:

`www.unipraxis.com/solutions.cgi?id=LogiCard`.

In the actual notification message, this URL will therefore be represented as:

`www.unipraxis.com/solutions.cgi?`

Variables in User Notifications for File Events

You can use variables when specifying user notification messages or smart tags.

Notification messages

When defining the text in a notification dialog for a file event you can use variables to customize the text content based on the circumstances of the control event. For example, if a control trigger displays a warning when users attempt to copy a particular Microsoft Office document to a removable drive, you can use the `%author%` variable to include the name of the file author in your notification message.

File variables used in this context only apply to files detected by Data In Motion triggers where the control action is set to Block, Warn or Inform.

Smart tags

You can also use these variables to specify smart tags. In many cases, they are better suited for use as smart tags than in notification messages. Smart tags allow you to categorize scanned or captured file events and are stored with the events on the CMS.

Some variables can only be used when specifying smart tags.

File variables used in this context apply to files detected by any Data In Motion or Data At Rest trigger.

Note: Variables are not case-sensitive. So, for example, you can type %URL% or %url% when defining a notification message.

The supported variables follow:

%accessed%

Displays the date and time when the file was last accessed. For NBA-captured files, it displays the date and time when the NBA reassembled the file.

For example, this smart tag value:

Last accessed:%accessed%

Generates this smart tag:

Last accessed:2009-06-22T13:34:44.460

%author%

(For Microsoft Office files only) Displays the file's Author property.

For example, this message in the policy:

You are not permitted to print documents written by %author%.

Displays like this in a notification message:

You are not permitted to print documents written by Spencer Rimmel.

%channel%

(For CA DataMinder Network-captured files only) Displays the type of activity, for example: WEB, WEBMAIL, EMAIL, FTP, IM or NEWS. This variable is typically used in smart tags to categorize captured events.

Only WEB, WEBMAIL, and EMAIL can appear in blocking notifications; captured events on other channels (such as FTP file transfers) cannot generate user notifications.

For example, this smart tag value:

Activity: %channel%

Generates this smart tag:

Activity: FTP

%created%

Displays the date and time when the file was created. For CA DataMinder Network-captured files, it displays the date and time when the CA DataMinder Network reassembled the file.

For example, this smart tag value:

File created: %created%

Generates this smart tag:

File created:2009-06-21T10:35:51.342

%dest%

Displays the machine name (if available) or IP address of the destination machine. For file uploads or files sent via IM conversations, the destination machine is a Web server.

For example, this smart tag value:

Destination: %dest%

Generates this smart tag:

Destination: 212.58.226.79

%device%

For files captured by the CFSA, this displays the name of the USB device. For files captured by the CPSA, this displays the printer name.

For example, this message in the policy:

You are not authorized to copy files to this device: %device%.

Displays like this in a notification message:

You are not authorized to copy files to this device: Unipraxis,DataPen 3.0,PMAP,,

%filename%

Displays the name of the file captured, scanned or imported by CA DataMinder. For example, this message in the policy:

You are not permitted to copy %filename%.

Displays like this in a notification message:

You are not permitted to copy Contact_Details.docx.

%host%

For files captured by CA DataMinder Network or imported files, this displays the machine that the file was ingested from (that is, the machine hosting the file).

For files captured by the CFSA or CPSA, this displays the machine hosting the CFSA or CPSA.

For example, this smart tag value:

Host computer: %host%

Generates this smart tag:

Host computer: ux-milano-xp

%MessageToUsers%

Displays the value of the Message To Users setting.

For example, you can forward blocked emails to a manager. You can also specify separate notification messages for the original sender and the manager. If the user policy specifies:

- This message for the 'Trigger/Message to Users' setting in the trigger:
References to %Keysting% are prohibited in corporate correspondence.
- This message for the 'System Settings/User Notifications/Forwarded E-mail Settings/Outgoing Body' setting:
The attached mail was blocked. The message displayed to the sender was "%MessageToUsers%".

Then, the forwarded email contains this message:

The attached mail was blocked. The message displayed to the sender was "References to Project Alpha are prohibited in corporate correspondence."

%modified%

Displays the date and time when the file was last modified.

For CA DataMinder Network-captured files, it displays the date and time when CA DataMinder Network reassembled the file.

For example, this smart tag value:

File modified: %modified%

Generates this smart tag:

File modified:2009-06-27T18:41:58.312

%path%

Displays the path to the file, excluding the server and the file name itself. For example, this smart tag value:

Found in: %path%

Generates this smart tag:

Found in: C:\Users\SRimmel\Documents

%protocol%

Available only for CA DataMinder Network-captured files. Displays the data transport protocol, such as HTTP-POST, HTTP-GET or HOTMAIL-ATTACH.

For example, this smart tag value:

Protocol: %protocol%

Generates this smart tag:

Protocol: HTTP_POST

Alternatively, this example message in the policy:

The following %protocol% file has been blocked.

Displays like this in a notification message:

The following HOTMAIL-ATTACH file has been blocked.

%size%

Displays the file size in bytes. For example, this smart tag value:

Bytes: %size%

Generates this smart tag:

Bytes: 11023

%source%

(Available for CA DataMinder Network-captured files only) Displays the machine name (if available) or the IP address of the source machine. For file downloads, the source machine is a Web server. For example, this smart tag value:

Source: %source%

Generates this smart tag:

Source: cn=unipraxis.com(231.38.126.79),cn=computers

%subject%

(Available for Microsoft Office files only) Displays the file's Subject property. For example, this smart tag value:

Subject: %subject%

Generates this smart tag:

Subject: Contact Details

%TriggerName%

Displays the value of the Trigger Name setting.

For example, if the user policy specifies this message for the 'Trigger/Message to Users' setting in the trigger:

This message or the associated attachment(s) you are attempting to send is in possible violation of a corporate intellectual property rights policy called "%triggername%".

Then it displays like this in a notification email:

This message or the associated attachment(s) you are attempting to send is in possible violation of a corporate intellectual property rights policy called "Patent Applications".

%URL%

Available only for certain CA DataMinder Network-captured files. Displays the destination URL for file transfers. Note that this information is not always available.

For example, this message in the policy:

Your file transfer to %url% has been blocked.

Displays like this in a notification message:

Your file transfer to http://ux-milano-xp/data/form_handler.asp has been blocked.

More information:

[Smart Tags and File Events](#) (see page 278)

Chapter 25: User Definitions

User definitions, also known as 'replaceable strings' are variables that can be referenced by any settings in the current user policy that have a text value (for example, trigger names, address lists, search text lists, messages to users). For example, you can define a 'Disclaimer' user definition and reference this as %Disclaimer% in any Trigger Name setting.

Example

For example, you can add a 'Disclaimer' user definition and set its value to:

Unipraxis distributes this document for informational purposes only.

You can then reference this definition as %Disclaimer% in any other policy trigger. For example, you can include this definition in the explanatory message that users see when their email is blocked, for example:

"Your email has been blocked because it does not include the mandatory corporate disclaimer: %Disclaimer%"

To set up a user definition

1. Open the policy you want in the Administration console.
2. In the Policy Editor screen, browse to the System Settings folder.
3. In the Definitions policy folder, select the User Definitions setting and the User Definition you want to configure.
4. Enter a name for the user definition, such as 'Disclaimer'.
Note: This name is case sensitive and must not contain spaces or a percentage symbol (%).
5. Enter a value for the definition, such as:
Unipraxis distributes this document for informational purposes only.
6. This user definition can now be referenced as a string value in any other policy trigger, for example, in a Message To Users setting:
"Your email attachment has been blocked, as it is missing its mandatory corporate disclaimer: %Disclaimer%"

Notes:

- If you inadvertently define multiple User Definitions with the same name, then any duplicate definitions are ignored and an error is written to the Activity log.

User definitions can themselves contain variables specified by other user definitions. Ensure that you do not create circular references. For example, if User Definition 1 references User Definition 2, User Definition 2 must not reference User Definition 1.

Chapter 26: Definitions

The system settings include a Definitions subfolder. Settings in this subfolder let you specify various definitions, such as internal email address patterns, archive file extensions, and 'user definitions' (variables defined by you, such as a list of banned phrases).

Such user definitions can be referenced by any setting in the current policy that takes a text value (such as trigger names, address lists, search text lists, and messages to users). This can save time and ensure consistency if a policy contains many settings that use the same.

Example

For example, you can add a 'Disclaimer' user definition and set its value to:

Unipraxis distributes this document for informational purposes only.

You can then reference this definition as %Disclaimer% in any other policy trigger. For example, you can include this definition in the explanatory message that users see when their email is blocked, for example:

"Your email has been blocked because it does not include the mandatory corporate disclaimer: %Disclaimer%"

Chapter 27: Troubleshooting User Policies

Because CA DataMinder deployments can be highly complex, monitoring thousands of users, problems inevitably arise. Typically, a user policy seems to be malfunctioning; emails that should be blocked are allowed to continue, while emails that are benign are inexplicably causing triggers to fire.

How can you pinpoint the cause of these problems, and how do you resolve them? Our experience on customer sites has proved that most of these problems are easily fixed by systematically eliminating the most likely causes until you arrive at the root problem. In particular, many problems appear to be policy failures but are in fact caused by unrecognized email addresses. This section describes how to troubleshoot suspected policy problems by identifying the most common points of failure.

This section contains the following topics:

[Triggers Are Not Firing As Expected](#) (see page 367)

[A Policy is Not Working or Cannot Be Edited](#) (see page 369)

Triggers Are Not Firing As Expected

Symptom:

A user policy seems to be malfunctioning and triggers are not firing as expected. For example, emails that should be blocked are allowed to continue, or emails that are benign are inexplicably causing triggers to fire.

Solution 1: Confirm that the user is not exempt from policy

If a user account has inadvertently been exempted from policy, CA DataMinder does not apply policy to that user. *Exempt users* are users who have a CA DataMinder account on the CMS but who are exempt from policy. That is, CA DataMinder does not monitor email, web or file activity for policy-exempt users.

To check a user's policy exemption status

1. Log on to the Administration console using an account that has the 'Users: Edit the user hierarchy' administrative privilege.
2. Expand the User Administration branch and select the user with the problem policy.
3. Click Tools, Set Policy Exemption.

The Select Policy Exemption State dialog appears.

4. Verify that the Exempt From Policy check box is clear.

If the check box is selected, the user is exempt from policy and CA DataMinder does not apply policy triggers.

Solution 2: Confirm that the latest policy version is being used

If the correct user policy is being applied but there is still a problem, it is possible that the wrong version of that policy is being applied. Typically, updated policy versions are replicated to client machines automatically. If the affected user is not logged on or logged on twice, there can be a short delay during which the latest policy changes have not yet been sent down to all endpoint agents on users' workstations.

To identify the assigned and reported versions

1. Log on to the Administration Console as the primary administrator.
2. Select the user under User Administration.

The attributes in the right-hand pane show the policy version, for example: 1.2.3.4. If the user is currently logged on to CA DataMinder, both assigned and reported policy versions are displayed.

3. Compare the policy version number assigned by the CMS with the version reported by the client machine.
4. If the wrong policy version is being applied, manually replicate the updated version to all child machines.

To replicate the user policy

1. Log on to the Administration Console as the primary administrator.
2. Choose Tools, Replicate Changes from the menu bar.

The latest policies are replicated down to all child machines.

Solution 3: Check for common errors in the user policy

If you have verified that the correct version of the correct user policy is being applied, but there is still a problem, you now need to check the policy settings.

For example, are your Search Text settings configured correctly? The syntax for search text expression can be complex. You can test whether your triggers are looking for the correct text by sending test emails.

Solution 4: Contact Technical Support

If you have confirmed that the correct user policy is being applied but you are unable to identify any obvious errors in the policy itself, contact [support](#). Be prepared to supply helpful diagnostic files, such as:

- XML exports of the relevant policy files: In the User Policy Editor, choose File, Export Policy XML.
- WgnCheck dump files.
- Log files such as the CA DataMinder Express infrastructure log file, wgninfra.out.

A Policy is Not Working or Cannot Be Edited

Symptom:

If a policy stops working or cannot be edited, it may be corrupt. When you try to edit a corrupt policy, an error message indicates a failure to load a policy from the database.

A corrupt policy can manifest itself in various ways:

- A corrupt **machine policy** causes all CA DataMinder operations to stop on that machine.

For example, any browser or e-mail integration features and the infrastructure will stop working (see below). If a common client machine policy or a common gateway policy is affected, this will affect all client machines or all gateways respectively.
- If a **user policy** is corrupted, all policy settings stop working.

In particular, triggers will not activate. It may also cause e-mail and Web applications to be disabled, depending on how the Infrastructure Failure setting is configured (see below). The position of the associated user or group within the user hierarchy is also important because any child policies will also be adversely affected.

Solution:

The Infrastructure Failure setting controls how CA DataMinder responds when the infrastructure fails to start. Find this setting in the user policy System Settings, Initialization folder. For example, you specify that only CA DataMinder is disabled, or you can also disable all browser and e-mail applications integrated into CA DataMinder (this prevents users running their browser or e-mail applications until the infrastructure restarts).

To overcome a corrupt policy

1. First, you must identify the .BLB file containing the corrupt policy. To identify the corrupt policy, run:

```
wgninfra -exec wigan/infrastruct/policy/PolicySetup PolicyCheck
```

Note: These commands are case-sensitive.

2. This command forces CA DataMinder to examine each policy file on the CMS. If a corrupt policy is detected, an identifying entry is written to the latest System log.
3. When you have identified the corrupt policy and the associated file, please contact CA Technical Support for further advice: <http://ca.com/support>.

Chapter 28: Best Practices

This section describes the best practices for refining CA DataMinder policies. These best practices have been honed by CA's own policy consultants and subject matter experts after many years spent deploying CA DataMinder on customer sites.

This section contains the following topics:

[Refine Your Policies in a Lab](#) (see page 371)

[Matching a Document Classification](#) (see page 372)

[Excluding Emails By Sender](#) (see page 373)

[Excluding Emails By Subject](#) (see page 375)

Refine Your Policies in a Lab

Before deploying CA DataMinder in a production environment, you will need to refine your user policies to ensure that they work you want them to and to minimize the number of false positives (that is, occasions when a file or email caused a trigger to fire needlessly).

Typically, you refine your policies in a lab using a pool of test data (emails and files) that you repeatedly import into CA DataMinder while applying policy. After each import operation is complete, you compare the trigger rate with that of the previous operation (did triggers fire more frequently or less frequently?) and refine your policies as necessary. Over several sessions, you are able to assess the effectiveness of any policy changes.

We recommend that your lab setup includes an endpoint agent to allow interactive, real-time testing. For example, if your policies use long, complex keystrokes to detect key words or phrases, it can be extremely useful to run real-time tests to iteratively verify the proper performance of these policy settings.

Matching a Document Classification

Most policy refinement typically involves your document classifications. And most document classifications are heavily based on Parameter 3 and, possibly, Parameter 2.

- **Parameter 3** defines a list of positive-indicator words or phrases. If any are present, this increases the probability that the document matches the specified classification. CA DataMinder raises the document coefficient by +1 for each occurrence of a listed word or phrase.
- **Parameter 2** defines a list of required words or phrases, one of which must be present for CA DataMinder to confirm a document classification. This is useful if you need to detect difficult language or common terms. These terms act as a policy pre-qualifier; a trigger cannot fire unless at least one of term is present. If validated, this parameter raises the document coefficient by +1. In effect, this parameter specifies a logical OR condition.

For full details about all document classification parameters, search the Administration console online help.

Excluding Emails By Sender

An organization often generates emails from one or more general sender mailboxes. These emails occasionally trigger policy and are usually of no interest to the reviewers. It therefore makes sense to exclude these senders from policy. There are several approaches:

- **Create a custom CA DataMinder account for the sender and disable policy**

If the sender matches an existing CA DataMinder user account, you can simply disable policy for the sender. You may therefore want to create a custom CA DataMinder user to represent one or more of the system mail senders.

For the example email above, you could create a CA DataMinder user called AutoSenders and assign the address announcement@globalcorp.com to this account. You can now disable policy for this user by editing the user's policy directly or editing policy for the group that contains this user.

- **Exclude senders from policy by using Data Lookup commands**

If it is not practical to include the sender in the hierarchy, you can use data lookups to exclude the sender. This is normally the case when the sender is external. Depending on the scope of the excluded addresses, there are several valid approaches.

- If the sender has a specific address, use:

```
msgattr where %sender% IS {"announcement@globalcorp.com"}
```

If you want to exclude a specific *internal* sender, then the above command may not be sufficient. Typically, you need to specify the sender's EX address (this is the protocol used internally by Microsoft Outlook). For example:

```
msgattr where %sender% IS {"o=globalcorp/ou=us/cn=announcement"}
```

Alternatively, use the following example to cover all possibilities:

```
msgattr where %sender% IS ANY  
{"announcement@globalcorp.com", "/o=globalcorp/ou=us/cn=announcement"}
```

Note: The Retrieve Full Sender Details For Emails? setting in the user policy is the key determinant on how sender addresses are handled. By default, this setting is True, meaning that CA DataMinder retrieves all the sender's address aliases.

- If you want to exclude a few specific sender addresses, you can specify a comma separated list of addresses:

```
msgattr where %sender% IS {"announcement@globalcorp.com",  
"hr@globalcorp.com", ...}
```

- If there are many potential sender addresses that you want to exclude, and this list is used by multiple triggers, we recommend a user definition:

```
msgattr where %sender% IS ANY {"%ExcludedSenders%"}
```

Here, %ExcludedSenders%" is a user definition, included in each user's policy, that specifies a long list comma separated list of addresses.

- For very large lists of external addresses, such as spam senders, you can also use a custom CA DataMinder user account in a custom user group. You must then assign all the spam sender addresses that you know about to that user account. This allows you to use a User Attribute lookup command to exclude members of this custom group from policy. In the example below, the custom CA DataMinder user is a member of the WhiteList user group:
`userattr with %sender% WHERE Wgn.Group IS NOT {"WhiteList"}`

Note: When refining your Outgoing Email triggers, external senders are represented in the CA DataMinder user hierarchy by the ExternalSender user account. If you want to apply Data Lookup filters to external senders, make sure you edit the triggers for the ExternalSender user

Excluding Emails By Subject

In addition general sender mailboxes that issue emails that require policy-exemption, organizations often want to ignore emails with specific subjects. This is easily achievable by specifying lists of excluded words or phrases (that is, any email containing these words or phrases is excluded from policy). The trigger settings for this approach are:

Search Which Sections or Documents?

Set this to 'Subject'.

Which Search Text List?

Set this to 'Use the Excluded List'.

Excluded Search Text

Add the words or phrases you want to exclude. Any words or phrases added to here and which are subsequently detected in an email's Subject will exclude that email from policy (no triggers will fire), even if the email matches a document classification. Consider these four approaches:

- In the example email, you could add the term **Company Newsletter** to the Excluded Search Text list. This would eliminate the email, but could also create a policy loophole because any email with 'Company Newsletter' in the subject would be excluded from policy.
- A tighter approach would be to append a month reference to the excluded phrase:
Company Newsletter – {January|February|...|December}.
- To further close the loophole, you could add year reference:
Company Newsletter – {January|February|...|December} %digits(2000,2100)%.
- Because users will often forward or reply to a message, simply excluding the original subject, however detailed, may still be too loose. For example, if a user forwards a message, 'FW:' is typically appended to the original Subject. To prevent such replies or forwarded emails from being excluded, you can augment the exclude text with variables to stipulate that any text match must occur at the start of the subject line:
Company Newsletter – {January|February|...|December} %digits(2000,2100)%
%precededBy% %ENDBUF%

In this example, emails with "Company Newsletter..." as the subject are excluded from policy, but emails with a subject such as "RE: Company Newsletter.." are not.

When refining policies in a typical CA DataMinder enterprise, it is common for there to be numerous excluded subjects such as these, and for these excluded subjects to feature across multiple triggers. In such situations, the best approach is to create a User Definition called 'ExcludedSubjects' and add all your excluded terms to this definition. You can then use %ExcludeSubjects% in each trigger's Excluded Search Text setting.

Note: This method is less secure than excluding by sender because any user who knows the excluded phrases can deliberately add them to their e-mail to circumvent policy.

Chapter 29: Example User Policy

This section shows example settings for a policy trigger and document classification.

Corporate rules typically prohibit employees from disclosing sensitive network information such as usernames or passwords. In this example, a policy trigger and document classification are configured to detect emails that contain these details.

This section contains the following topics:

[Example Trigger Settings](#) (see page 378)

[Example Document Classification](#) (see page 380)

Example Trigger Settings

This example shows settings for an email trigger configured to detect messages or attachments that contain usernames or passwords. The main analysis is performed by the specified document classification (see the following section).

Setting: Trigger Name

Value: Sharing of Usernames and Passwords

Setting: Policy Class

Value: Sharing of Usernames and Passwords

Setting: Severity

Value: 50

Setting: Smart Tags

Value: Classification

Setting: Which Address List?

Value: Use the Excluded List

Setting: Included Addresses

Value: *

Setting: Excluded Addresses

Value: <none>

Setting: Ignored Addresses

Value: <none>

Setting: Trigger Name

Value: Sharing of Usernames and Passwords

Setting: Which Document Classification?

Value: Classification 79 (Sharing of Usernames and Passwords)

Setting: Check Which Items?

Value: Subject, body and attachments

Setting: Which File Name List?

Value: Use the Included List

Setting: Included File Names

Value: *

Setting: Excluded File Names

Value: <none>

Setting: Encryption Filter

Value: All emails

Setting: Digital Signature Filter

Value: All emails

Setting: Search Which Sections or Documents?

Value: Subject

Setting: Which Search Text List?

Value: Use the Excluded list

Setting: Included Search Text

Value: <none>

Setting: Excluded Search Text

Value: %GlobalSubjectExcludes%

Setting: Which Email Sources?

Value: All

Setting: Data Lookup Command

Value: <empty>

Setting: Data Lookup Failure Mode

Value: Do not fire trigger

Setting: Minimum retention (Days) - Authorized Activity

Value: 0

Setting: Minimum retention (Days) - Prohibited Activity

Value: 0

Setting: Control Action

Value: Control Action 2 (Warn)

Setting: Message To Users

Value: This message or the associated attachment(s) you are attempting to send is in possible violation of a corporate security policy called "%triggername%".

Possible recommended actions that can be taken to eliminate or mitigate risk:

1. Remove words or phrases that you may consider being in violation of this policy before sending the message.
2. Do not send message.
3. Password Protect or use appropriate encryption policy.
4. Confirm that all recipients are approved for this communication.

Contact %NameOfSecurityOfficer%, security officer on %ExtensionOfSecurityOfficer% if you have questions regarding this message.

Example Document Classification

This example document classification is designed to detect occurrences of usernames or passwords in emails and files. It only uses parameters 3, 4, 5 and 6.

Parameter 3 contains the keystings (text items) that underlie the document classification. Each match raises the document score by 1.

Parameters 4 and 5 define the words or phrases that indicate a non-match. In this example, these terms are mainly defined in the %GlobalDocumentExcludes% user definition.

Parameter 6 specifies the minium score needed to fire the trigger.

Setting: Name

Value: Sharing of Usernames and Passwords

Setting: Configuration

Value: Generic

Setting: Parameter 1

Value: <none>

Setting: Parameter 2

Value: <none>

Setting: Parameter 3

Values: The policy list setting contains the following items:

```
%!-- Usernames --% Access|Acces|Acess Nm|Name|Names|ID|IDs
%!-- Usernames --% Sign On|Ons|In|Ins|Into|Onto {ID|IDs}}{?}
%!-- Usernames --% Use|User|Users Nm|Nms|Name|Names|ID|IDs
%!-- Usernames --% Use|User|Users
LogOn|LoggOn|LogOns|LoggOns|LogIn|LoggIn|LogIns|LoggIns ID|IDs}}{?}
%!-- Usernames --% Log|Logg{{
}}\p}{?}Nm|Name|Names|In|Ins|On|Ons|Into|Onto{{ }}{ID|IDs}}{?}%
%!-- Usernames --% User { : | Is}
%!-- Password --% PASS { : | = | Is | for | to} %PrecededBy% %WhiteSpace%
%!-- Password --% { {%#P/{W|N|#|{No}}{s}{?}%} | {%#P\\{W|N|#|{No}}{s}{?}%}
%PrecededBy% %WhiteSpace% }
%!-- Password --% Access|Acces|Acess Code|Codes
%!-- Password --% {%#Pass|Pas|P{{
}}\p}{?}Word|Words|Wrd|Wrds|Code|Codes%
```

```
%!-- Password --% {%+MatchCase% PIN | PINs | PINS %-MatchCase%}
{{ { Conf | Conference }%false%}|%ANY%}[\\,15] {%#\d[3\\,7]%}
{{ %PrecededBy% {{ %any%[\\,5] Conf | Conference }%false%}[?] %WhiteSpace%}}
```

```
%!-- Password --% Personal|Per|Pers {Identification|{I.D.}|{I.D}|ID}
Number|Numbers|Num|Nums|Numb|Numbs|No|Nos|#
```

```
%!-- Password --% PSWD | PSWDs %PrecededBy% %WhiteSpace%
```

```
%!-- Password --% PW | PWs | PWD | PWDs %PrecededBy% %WhiteSpace%
```

Note: You can use syntax such as %!--Password--% to add comment to your policy settings..

Setting: Parameter 4

Values: The policy list setting contains the following items:

```
%-matchpunct% password* %any%[,5] {non-public} | {non public} information in
your
```

does not require a password

Setting: Parameter 5

Values: The policy list setting contains the following item:

```
%GlobalDocumentExcludes%
```

Setting: Parameter 6

Value: The policy list setting contains the following items:

```
minscore(2)
```

```
extract(1,2,3,8)
```

Setting: Parameter 7

Value: <none>

Setting: Parameter 8

Value: <none>

Setting: Parameter 9

Value: <none>

Setting: Parameter 10

Value: <none>

Appendix A: Search Text Syntax

CA DataMinder uses the term 'search text' to mean the key words and phrases that you want a trigger to detect. Triggers can detect 'search text' in emails, files, Web events and IM conversations.

Trigger settings such as 'Included Search Text' let you define the search text for a specific trigger. Search text can be an exact phrase or it can include wildcards, alternatives, and many special variables for matching specific types of information (such as URLs, email addresses, or social security numbers).

The following sections describe the supported search text variables and the required syntax.

For general usage instructions, see [Detecting Key Text](#) (see page 133).

This section contains the following topics:

[Special Characters](#) (see page 384)

[Wildcards](#) (see page 385)

[Subexpressions and Logical Operators](#) (see page 386)

[Word and Symbol Variables](#) (see page 387)

[Number and Money Variables](#) (see page 390)

[Email Address and URL Variables](#) (see page 392)

[Repeat Expressions](#) (see page 393)

[Punctuation Variables](#) (see page 395)

[Spacing Variables](#) (see page 396)

[Comments](#) (see page 397)

[Per Character Matching](#) (see page 398)

[User-defined Variables](#) (see page 400)

[Matching Forwards and Backwards](#) (see page 405)

Special Characters

The following characters have special meaning:

{ } | [] % ? * \

To search for literal occurrences of these characters, you must prefix them with a \ backslash.

Note: Forward slashes are not special characters and do not need a backslash prefix. For example, you need only type 24/7 to detect '24/7'.

Examples

What next\?

If this example is part of an Included list, the trigger activates whenever CA DataMinder detects:

What next?

24*7

If this example is part of an Included list, the trigger activates whenever CA DataMinder detects:

24*7

The files are located in the \\Sales directory

If this example is part of an Included list, the trigger activates whenever CA DataMinder detects:

'The files are located in the \Sales directory'.

Note: To search for literal occurrences of backslash characters, you must still prefix them with a further backslash. This is why you must type \\Sales to detect '\Sales'.

The domain you need is: unipraxis\srimmel

If part of an Included list, the trigger activates whenever CA DataMinder detects:

'The domain you need is: unipraxis\srimmel'

More information:

[Special Characters](#) (see page 137)

Wildcards

You can use wildcard characters `*` and `?` when you define a list of trigger words or phrases.

`?`

A `?` wildcard matches any digit, letter or punctuation character.

Example: *spen?er* matches names such as *Spencer* or *Spenser*.

Example: *ref???a* matches words such as *ref328a*.

`*`

A `*` wildcard matches any sequence of zero or more digits, letters or punctuation characters.

Example: *unipr** matches words such as *Unipraxis*.

Example: *holiday req** matches phrases such as *holiday request*.

If the search expression is simply `'*'`, the trigger fires if it detects anything.

Literal `*` and `?` characters

To search for literal occurrences of `*` and `?` characters, prefix them with a `'\'` backslash.

Example: *What next for Unipraxis\?* is needed to match *What next for Unipraxis?*

Example: *24*7* is needed to match *24*7*.

Subexpressions and Logical Operators

Subexpressions allow you to group together a section of the match, enabling you to specify repeats for whole sections of text, specify optional sections of text, or variations.

Subexpressions use the following syntax:

{subexpression}

Curly brackets delimit sub expressions. That is, they group together two or more words. You can use sub expressions to specify complex patterns of search text. You also need curly brackets if the word contains numbers, even if it is a single word.

Example: *Unipraxis* does not need brackets.

Example: *{Unipraxis Securities}* does need brackets.

Example: *Please could you|{your firm}|Unipraxis forward further information.*

Example: *The new slogan is {Go2Market}.*

Note: Curly brackets do not affect user performance. For ease of maintenance, you can entirely enclose a search expression in curly brackets.

a|b

The pipe symbol "|" is an OR operator.

Example: *spencer|frank* matches *spencer* or *frank*.

%FALSE%

Aborts all matching immediately for this expression. This subexpression can be used to specify a negation.

Example: The expression *1234{+%false%}[?]* matches *1234* but not *1234+*

In this example, the search matches *1234* initially. It then looks for a plus symbol (+). If one is found, the *%false%* variable forces the match to abort. If a plus symbol is not found, the search continues matching because the *{+%false%}* subexpression is optional.

Word and Symbol Variables

Use the following search text variables to detect words, phrases and symbols.

%ANY%

Matches any symbol (word, number, or punctuation).

Example: *your %any%[,5] report* matches *your 2011 sales report*.

%WORD%

Matches a single whole word. A word can only contain letters, and no numbers or symbols.

Example: *your %word%[,5] balance* matches *your bank account balance* but does not match *your request. The balance* because "request." includes a period and so is not classed as a word.

%+WORD%

Only matches words. That is, the matched text must only include letters.

Example: *%+word% ??* can only return words with two letters so if it is matched against *see you at 11*, it returns *at*.

%-WORD%

Disables *%+WORD%*

Example: *%+word% account *[,5]%-word% 123456* matches *account number is 123456*.

%STRING%

Matches the sequence of characters until the next white space, including punctuation.

Example: *in the %string% folder matches in the \\ux-milano\sales\prospects folder.*

%SENTENCE%

Matches any text in a sentence up to the next period character. The match does not treat exclamation or question points as ends of sentences.

Example: *merger %sentence% problems matches merger still faces problems.*

%SAMESEN%[n,m]

Matches any text within a specified number of words, up to the next period, question or exclamation point. You can limit "word1 %SameSen% word2" to match within [n,m] words, where n is the minimum and m the maximum number of words that can match between word1 and word2.

Note: %SameSen% is a user-defined variable that is only available in the Foundation Policy Pack or iConsole Standard Policies.

Examples:

quick %SameSen%[,5] dog matches The quick brown fox jumped over the dog. and quick dog. It does not match John was quick. The dog was brown.

merger %SameSen% problems matches merger still faces problems!

%ENDBUF%

Matches to the end of the text buffer, where 'buffer' refers to the section of text being searched. Typically, this variable matches to the end of the email or document or, if matching backwards, to the start of the email or document.

Example: *they lived %endbuf% matches they lived happily ever after.* if this phrase occurs at the end of the document.

%CAP%

Matches any word starting with a capital letter.

Example: *%cap% %cap% matches Spencer Rimmel but does not match spencer rimmel.*

%+CAP%

Must begin with a capital letter.

Example: *%+word% %+cap% ?* returns only single letter words in upper case, so if it is matched against *A man in a hurry*, it returns only *A*.

%-CAP%

Disables %+CAP%.

%+matchCase%

Specifies case-sensitive matching.

By default, when triggers search for key words or phrases, these searches are case insensitive. Use this variable to switch to case-sensitive matching.

Example: *%+matchCase%Shadow Chancellor* only matches *Shadow Chancellor*.

%-matchCase%

(Default) Specifies case-insensitive matching. Use this variable in conjunction with *%+matchCase%* to revert back to case-insensitive matching.

Example: *%-matchCase%Shadow Chancellor* matches *Shadow Chancellor* or *shadow chancellor*.

%x1234%

Specifies the decimal code of a single Unicode character.

Example: *%x169%* matches the copyright symbol ©.

%PUNCT%

Matches any sequence of punctuation symbols.

Example: *ID%punct% 1234* matches *ID: 1234*.

Example: *%-matchSpace%ID%punct% 1234* matches *ID: 1234* and *ID-1234*.

%+PUNCT%

Only matches punctuation symbols. That is, the matched text must include punctuation symbols.

Example: *%+punct% ???* matches *!!!*

%-PUNCT%

Disables *%+PUNCT%*.

Example: *%+punct% ???%-punct%???* matches *!!!abc*.

Number and Money Variables

Use the following search text variables to match numbers and money amounts.

Numbers

%DIGITS%

Matches a sequence of digits.

Example: *invoice %digits%* matches *invoice 60340*.

%DIGITS[X,Y]%

Matches a sequence of digits, whose value is between X and Y.

Example: *%digits[100,200]%* matches any number from 100 through 200.

Example: *%digits[1,31]%/ %digits[1,12]%/ %digits[2005,2011]%* matches all DD/MM/YYYY dates from 2005 through 2011, for example, *17/2/2011*.

%INT%

Matches any integer.

Example: *%int%* matches *123* and *-123* and *123,000*. It does not match *123.4*.

%FLOAT%

Matches any number with a decimal point.

Example: *%float%* matches *123.45* and *-123.45* and *123,000.45*. It does not match *123*.

%NUMBER%

Matches any number, including numbers with decimal points or comma formatting.

Example: *Buy %number% units at %money% each* matches *Buy 100 units at £34.45 each* and *Buy 100 units at £1,150 each*.

%+NUMBER%

Must be a number.

Example: *%+number% ???* matches three digit numbers such as *123*.

%-NUMBER%

Disables *%+NUMBER%*.

Social Security Numbers

%SSN%

Matches a whole US social security number. That is, this variable identifies social security numbers both in *nnnnnnnnnn* format and in *nnn-nn-nnnn* format.

Example: *%SSN%* matches *123456789* and *123-45-6789*.

Note: CA DataMinder uses a sophisticated recognition process to cross-check against an imported system definition file. This file lists currently available social security numbers (the US Social Security High Group file). For details, see the *Administration Guide*; search for 'system definition file'.

%SSN_U%

Matches a whole *unformatted* US social security number in *nnnnnnnnnn* format.

Example: %SSN_U% matches 123456789 but not 123-45-6789.

%SSN_F%

Matches a whole *formatted* US social security number in *nnn-nn-nnnn* format.

Example: %SSN_F% matches 123-45-6789 but not 123456789.

Money and Credit Card Numbers

%MONEY%

Matches money amounts written using these formats: 99.00, \$99 or \$99.00, and USD 99 or USD 99.00. Equivalent formats for other currency codes and signs are also supported.

Example: %money% matches 6,217.50, \$250, and USD 3,501.

Example: %money% matches €250, £250, and ¥250.

Example: %money% matches EUR 250, GBP 250, and JPY 250.

%CCN%

Matches a whole credit card number, ignoring all white spaces. A match also eliminates common false positives and validates the number using the Luhn algorithm. The matched card number is returned in a label %CCN% for use in smart tags and user notification messages.

Email Address and URL Variables

Use the following search text variables to match email addresses and URLs.

%EMAIL%

Matches a whole SMTP e-mail address.

Example: *%email%* matches *spencer.rimmel@unipraxis.com*.

%EMAIL_PART%

Matches part of an e-mail address.

Example: *srimmel %EMAIL_PART%[*]* matches *srimmel@unipraxis.com* or *srimmel@unipraxis.co.uk*.

%URL%

Matches the whole URL.

Example: *%url%* matches *www.unipraxis.com*.

%+URL%

Must be part of a URL.

Example: *%+url% unipraxis* only matches *unipraxis* if it is part of a URL, such as in *www.unipraxis.com*. It does not match *The Unipraxis corporation*.

Repeat Expressions

To match against repeated words or subexpressions, use square brackets `[]` after a word. This syntax has the following format:

[*]

Matches any number of times, including zero.

Example: The expression `a b[*] c` matches both `a b b c` and `a c`.

[+]

Matches one or more times.

Example: The expression `a b[+] c` matches `a b b c`, but not `a c`.

[?]

Matches zero or once. That is, the repetition is optional.

Example: The expression `a b[?] c` matches `a b c` and `a c`, but not `a b b c`.

[N]

Matches N times, where N is a number.

Example: `a b[2] c` matches `a b b c`, but not `a b b b c`.

[N,]

Matches at least N times.

Example: `a b[2,] c` matches `a b b c`, but not `a b c`.

[,N]

Matches a maximum of N times.

Example: `a b[,2] c` matches `a b b c`, but not `a b b b c`.

[N,Z]

Matches from N to Z times.

Example: `a b[1,3] c` permits b to be repeated between one and three times. So this expression matches `a b b c` but not `a b b b c`.

Greedy matching

By default, search text matching is 'non-greedy'. That is, the search stops as soon as it finds a match. For example, if the expression `a[+]` is matched against `a a a a b` it returns `a`. The trigger fires as soon as it detects the first 'a'.

However, you can make a search 'greedy' so that it returns all matching occurrences. For greedy matching, the syntax has the following format:

[+g]

Continues to match one or more times.

Example: When `{many}[+g]` is matched against `many many times`, it returns `many many`.

Example: When `b a[+g]` is matched against `b a a a a`, it returns `b a a a a`

[*g]

Continues to match any number of times, including zero.

Example: When `b a[*g]` is matched against `b a a a a`, it returns `b a a a a`

[?g]

Matches zero or once.

Example: When `b a[?g]` is matched against `b a a a a`, it returns `b a`

[M,g]

Continues to match at least M times.

Example: When `b a[2,g]` is matched against `b a a a a`, it returns `b a a a a`

[,Mg]

Matches a maximum of M times.

Example: When `b a[ ,3g]` is matched against `b a a a a`, it returns `b a a a`

[M,Ng]

Matches from M to N times.

Example: When `b a[2,4g]` is matched against `b a a a a`, it returns `b a a a a`

Punctuation Variables

By default, a trigger matches punctuation when searching for key words or phrases, so *Unipraxis Win!!* matches *Unipraxis Win!!* but not *Unipraxis Win!* or *Unipraxis Win*. However, you can disable punctuation matching if you require more flexible matching. This can arise if your key words or phrases are frequently used with incorrect or inconsistent punctuation.

You can enable or disable punctuation matching with the following variables.

%+matchPunct%

(Default) Matches punctuation.

Example: The search expression is `%+matchPunct%Security: Breach` but the trigger detects *Security Breach*. This time, no match is confirmed.

%-matchPunct%

Ignores punctuation.

Example: If the search expression is `%-matchPunct%Security: Breach`, it returns *Security: Breach* even if the trigger detects *security breach*. This ensures that CA DataMinder triggers ignore all punctuation characters when looking for references to security breaches.

Spacing Variables

CA DataMinder matches spaces between words. Such spaces create a single, composite search term. So if the search text is *unipraxis solutions*, the trigger confirms a match if it detects the phrase *unipraxis solutions*. But by default, CA DataMinder ignores other spaces when searching for key words or phrases. These other spaces include tabs, line breaks, and spaces next to numbers or punctuation.

However, you can enable 'other space' matching if you require more flexible matching. You may want to do so if your key words or phrases are frequently used with consistent spacing. But be aware that matching against spacing can slow a trigger when it analyzes an email or file. It is only required for the most precise text searches that must match spacing exactly.

You can enable or disable space matching with the following variables.

%+matchSpace%

Matches spacing.

Example: The search expression is `%+matchSpace%Unipraxis (UNI15)` but the trigger detects *Unipraxis (UNI 15)*. This time, no match is confirmed.

%-matchSpace%

(Default) Ignores spacing.

Example: An email trigger that needs to detect all references to *Unipraxis (UNI15)*. However, some emails may refer to *Unipraxis (UNI 15)*. If you set the search expression to `%-matchSpace%Unipraxis (UNI15)`, it detects both references. That is, it returns *Unipraxis (UNI 15)* if the trigger detects *Unipraxis (UNI 15)* and it returns *Unipraxis (UNI15)* if the trigger detects *Unipraxis (UNI15)*.

Note: Any number of spaces is matched to a single space.

%whitespace% or %space%

Matches the space between elements in a word or phrase.

Example: `125%whitespace%-%whitespace%Taunton` matches against identifiers that explicitly contain spaces such as *125 - Taunton*. This example does not match against *125:Taunton*.

Note: These variables are only needed to match spaces between elements such as punctuation characters. CA DataMinder automatically matches spaces between words, so the simple search expression *125 Taunton* matches '*125 Taunton*'. (A word is any sequence of letters. Words do not include numbers or other characters.)

%joined%

Matches if the words or elements such as punctuation are adjacent.

Example: `125%joined%:%joined%Taunton` matches against *125:Taunton* but not *125- Taunton*.

Comments

You can include comments in any search expression. This is useful in complex expressions. Comments are marked with the following syntax:

%!-- ... --%

Identifies a comment.

Example: *%!-- Validates the number format --%*

Per Character Matching

By default, searches match against whole words. To enable a search to match against individual characters, use the following variables.

%# ... %

Matches the contained expression on a per character basis.

\a

Matches any single letter. See the examples below.

Example: `%#\a\123%` matches *GB123*.

\d

Matches any single digit (0-9).

Example: `%#GB\d\d%` matches *GB123*.

Example: When `%#ab{\d\d\a}{+g}%` is matched against *ab11a22d33f*, it returns *ab11a22d33f*. The `[+g]` indicates 'greedy matching'.

Example: When `%#{\d\d\}{\d\d\d} \d\d\??%` is matched against *Phone: 020 8686 3313 ; Id: 0a0 86bc*, it returns *020 8686* and *0a0 86bc*. The `??` wildcards match any character.

Example: When `%#{d[3,] }[3]%` is matched against *Phone: 020 8686 3313 ; Id: 0a0 86bc*, it returns *020 8686 3313*.

\l

Matches any single letter or digit.

\p

Matches any single punctuation character.

Example: `%#cn\p\d\d\d \a\d%` matches *cn:123 A3* and *cn-123 A3*.

\f

Aborts all matching immediately for this expression.

?

Wildcard. Matches any single character. See [Wildcards](#) (see page 385).

Space

A space in the search text expression matches spaces between words or other elements.

Example: `{contact list}` matches *contact list*.

Example: `%#ID \d\d\d%` matches *ID 123*.

Character ranges**[[a-z]]**

Matches any character between *a* and *z*.

Example: When `%#[[0-9]][4][[def]]%` is matched against *order: 7638f*, it returns *7638f*.

[[abc]]

Matches *a* or *b* or *c*.

Example: When `%#[[0123456789]][4][[def]]%` is matched against *order: 7638f*, it returns *7638f*.

Example: `%#[[0-9abcP-R]]%` matches any single character that is either: a digit between *0* and *9*; *a* or *b* or *c*; or any upper case letter between *P* and *R*.

[[^abc]]

Matches any character except *a* or *b* or *c*. Spaces are also excluded.

Example: When `%#[0-9][[^0-9]]%` is matched against *order: 0a 5u 12*, it returns *0a 5u*. The final element, *12*, is excluded because the search text expression explicitly excludes two consecutive digits.

More information:

[Repeat Expressions](#) (see page 393)

[Subexpressions and Logical Operators](#) (see page 386)

[Matching Forwards and Backwards](#) (see page 405)

User-defined Variables

You can search for specific text and, if found, assign that text to a custom variable. Any part of the matching text can be extracted and stored as a user-defined variable. You can then use the custom variable in smart tags and user notification messages.

Simple User-defined Variables

Use the following syntax to create custom variables.

%<MyVariable>%<search text>%</MyVariable>%

Matches any search text enclosed by the %<MyVariable>% tags and saves it to a variable %MyVariable%.

<MyVariable> can be any text. Variable names are case-sensitive. Variables must be terminated. That is, they must have a closing %</>% tag.

<search text> can be any word or phrase, and can include other variables.

Example: %<User_ID>% %#\a\a\a\a\d\d#% %</User_ID>% detects any *aaaaann* identifier such as *rimsp02* and saves it to a custom variable named %User_ID%.

Example: Here, the %<User_ID>% variable is incorporated into a user notification message: *Your email has been blocked. It includes a reference to User %User_ID%.*

Multiple and Overlapping User-defined Variables

You can create multiple user-defined variables from a single match, and variables can be overlapping. For example:

{Id = %<ID>% * %</ID>%}

When matched against *Id = 1234*, this search expression generates a single user-defined variable, %ID%. Its value is *1234*.

{%<ALL>% Id = %<ID>% * %</ID>%%</ALL>% }

When matched against *Id = 1234*, this search expression generates two user-defined variables:

%ALL% has a value of *Id = 1234*.

%ID% has a value of *1234*.

{%<START>%%<ALL>% Id %</START>% = %<ID>% * %</ID>%%</ALL>%}

When matched against *Id = 1234*, this search expression generates three user-defined variables:

%START% has a value of *Id* .

%ALL% has a value of *Id = 1234*.

%ID% has a value of *1234*.

Transforms

You can apply transforms to extracted text when you create a user-defined variable. This enables you to convert the extracted data into a standardized form, usually to make searching easier.

This attribute has the following syntax:

%<MyVar transform="{toLower|toUpper|stripWhitespace|onlydigits|onlyalpha}">%

Applies one of the transforms to the extracted text written to the %<MyVar>%.

toLower

Converts to lower case.

Effect: *GB123* transforms to *gb123*.

Example usage: This example ensures that values for the %<User_ID>% variable are always in lower case:

%<User_ID transform="toLower">% %#GB\d\d\d% **%</User_ID>%**

toUpper

Converts to upper case.

Effect: *gb123* transforms to *GB123*.

stripWhitespace

Removes all spaces

Effect: *abc 123* transforms to *abc123*.

onlydigits

Retains only numbers. Strips out letters and other characters.

Effect: *abc 123* transforms to *123*.

onlyalpha

Retains only letters. Strips out numbers and other characters.

Effect: *abc 123* transforms to *abc*.

TransformEx

You can perform more complex transforms using a conversion expression. This attribute can manipulate the extracted data in any number of ways. Use this attribute to add prefixes, take subsections, search and replace sections, and so on.

This attribute has the following syntax:

%<MyVar transformEx="X,...">%

Applies conversion expression X to the extracted text written to the %<MyVar>%.

You can apply multiple transforms and transform expressions can be specified. These are applied in the order in which they are stated.

Example: %<ID transformex="DOC_ID[\"\\%untilend\\%\",subsection=1:2]>% *
%</ID>%

Validation

Extra validation routines can be specified to a labeled region. Use this attribute to help ensure that the expression only matches if the labeled region also passes a validation test.

This attribute has the following syntax:

%<MyVar validate="{CCN|SSN}">% ...%/A>

Verifies that the extracted text written to the %<MyVar>% matches the specified validation routine.

The available validation routines are:

CCN

Matches a credit card number that is from 12 through 20 digits and passes the Lunn checksum.

Example: This expression validates whether the number written to the %<CreditCard>% variable is a valid credit card number:

*%<CreditCard validate="CCN">% * %%/CreditCard>%*

SSN

Matches an allocated US Social Security Number in the supplied highgroup file.

SSN requires access to the list of valid Social Security Numbers, as issued in the highgroup.txt file and available here at <http://www.ssa.gov/employer/highgroup.txt>.

In CA DataMinder, this file is installed in the CA DataMinder file system as SSN.dat.

In multiview, CA DataMinder looks for "highgroup.txt" in the same directory as multiview.exe.

Inside %CCN%

The %CCN% variable wraps up a large expression that: identifies Credit Card numbers; eliminates common false positives; validates the number using the Lunn algorithm; and removes all white spaces. The expression returns the number in a %CCN% variable that can be used in smart tags and user notification messages.

%CCN% expands to:

```
{%mark%
%digits% %return% %mark% %<<% {%digits%%false%}[?] %return% %mark% %>>%
%#{\d[13,20]}|{\d[3,4]{-| }\d[3,4]}[3,g]}%
{%digits%%false%}[?]
%return% %mark% %<<%
{%digits%| - |tel|tele|telephone|+|fax}|{{{#}|id|num|number}
{order|transaction|tracking|confirmation}}%false%}[?]
%return% %>>%
%<CCN validate="CCN" transform="onlydigits">% %digits%{- [?]%#\d[3,g]}[*g]
%</CCN>%
}
```

Inside %SSN%

The %SSN% variable wraps up a large expression that: identifies US Social Security Numbers; eliminates common false positives; validates the number using the highgroup.txt file; and removes all white spaces. The expression returns the number in a %SSN% variable that can be used in smart tags and user notification messages.

%SSN% expands to:

```
{%mark%
%digits% %return% %mark% %<<% {@|%digits%|\||{%joined%%word%}}%false%}
[?] %return% %mark% %>>%
%#{\d[9]}|{\d[3]{-| }\d[2]{-| }\d[4]}%
{@|%digits%|\||{%joined%%word%}}%false%}[?]
%return% %mark% %<<% {- |tel|tele|telephone|+|fax}%false%}[?]
%return% %>>%
%<SSN validate="SSN" transform="onlydigits">%
{%digits%{- [?]%digits%}[2]}|%\d[9]%
%</SSN>%
}
```

Matching Forwards and Backwards

By default, a search matches forwards through a document. That is, when matching against 'hello world' the trigger first looks for occurrences of 'hello' and then 'world' after it.

However, you can also match backwards through a document. Backwards matching can be useful if:

- You are searching for a sequence of words, but the only distinctive word is in the middle of the sequence.
- Your expression begins with *. For example, if matching against ** Rimmel*, the search can be extremely slow, as * matches every word.

Use the following syntax to specify the search direction:

%precededBy%

Return to the start of the match, and iterate backwards through the document.

Example: *fox jumped %precededBy% brown quick The* matches against *The quick brown fox jumped*.

Example: *Rimmel %precededBy% * ** matches against *welcome Mr. Rimmel*.

Example: *purchase order %sentence% %precededBy% %sentence%* matches against *This purchase order was raised by Spencer Rimmel*.

This last example matches the entire sentence by first matching *purchase order*, then matching up to and including the end of the sentence. The search then skips to the start of the match (that is, *purchase order*) and matches backwards until the period at the end of the previous sentence.

%forwards% or %>>%

(Default) Matches forwards.

Effect: If *fox jumped over* is matched against *The fox jumped over the log*, the cursor is initially before the start of the matched text. That is, the cursor is before *fox*. The cursor then moves to the first word (*fox*) and matches it. Now the cursor is over the word *fox*. Next, the cursor moves to the second word (*jumped*) and matches it, so the cursor is now over the word *jumped*. This process of MOVE then MATCH is repeated until a complete match is found, or not found.

%backwards% or %<<%

Matches backwards.

%mark%

Marks a position within the matched text.

%return%

Returns to a previously marked position.

%markReturn%

Marks this position, then returns to a previously marked position. You can use this to jump around the document.

Example

fox %mark% jumped %markReturn% %<<% brown quick The %return% %>>% over the lazy dog

This example matches *The quick brown fox jumped over the lazy dog*.

Briefly, the search marks and stores the current (cursor) position in the document, returns to that position later and continues to match in a different direction. In detail, the search expression carries out the following tasks:

1. It matches *fox*.
2. It adds marker (position 1) to *fox* using *%mark%*.
3. It matches *jumped*.
4. It adds marker (position 2) to *jumped*, and returns to previous position (position 1) using *%markReturn%*.
5. It iterates backwards using *%backwards%*.
6. It matches *brown quick The* backwards, returning *The quick brown*.
7. It returns to previous position (position 2) using *%return%*.
8. It iterates forwards using *%forwards%*.
9. It matches *over the lazy dog*

Glossary

assigned policy

This version of latest policy is assigned to a user or machine. This version is held on CMS and replicated automatically to the relevant gateway and client machine at intervals determined in the CMS policy.

classification

A *classification* is a set of parameters that define a specific type of document, for example, a sales proposal or a contract agreement.

CMS database changes

CMS database changes includes changes to policies and accounts, for both users and machines.

default group

New users who create their own accounts are added automatically to a *default group*. The default group is shown in bold in the Administration Console.

default items

List items inherited from the parent policy.

default values

Values copied from the parent policy.

embedded messages

An e-mail included inside another e-mail as an attachment.

replication intervals

Replication intervals are defined by Database Management settings in the CMS machine policy.

reported policy

The version number of a machine policy or user policy reported by a client machine when it logs on to the CMS.

search text

Search text refers to the key words and phrases that a triggers looks for in an email, attachment, file, Web page, or data submitted to a web site.

sequences

A *sequence* comprises of two or more items that were captured and are inseparably linked. An example is the series of Web pages captured on a single visit to a Web site.

warnings

A *warning* takes the form of a notification message in a warning dialog. You can define a separate message for each control trigger.

Index

—

__ (double underscore delimiter) • 349

A

actions • 24, 25, 27, 28

Address Book Lookup • 302, 303

address lists • 64, 67, 71, 73

advisories • 351, 357

C

classes, policy • 272

D

Data At Rest • 23, 27

Data Lookup • 295, 338

 address book lookup • 302, 303

 message attribute lookup • 304

 user attribute lookup • 297

 XML attribute lookup • 307, 309

document classifications • 30, 283

 parameter 6 • 288

 setting up • 284

E

emails, applying triggers to • 43

emails, encrypting • 167, 171

emails, which policy gets applied • 33

enforced folders • 51

exporting • 63

external addresses • 36, 37

F

files, applying triggers to • 43

files, encrypting • 204

files, which policy is applied • 34

fingerprinting • 212, 213

H

hidden folders • 53

hyphenated words • 138

I

IM events • 44

inheritance • 45, 46

inheritance, policy • 45, 46

internal addresses • 36, 37, 38

intervention options • 113

M

mapi lookup commands • 302, 303

msgvar lookup commands • 304

N

notification messages • 351, 357

P

PGP Portable, exempting devices • 203

policy

 editing in Administration console • 57

 how policy processing works • 41

 overview • 21

 whose policy gets applied? • 33

policy classes • 272

printed documents • 35

S

smart tags

 example • 277

 setting up • 276

system settings • 30

T

triggers • 21

U

user definitions • 62

user notifications • 351, 357

usrattr lookup commands • 297

V

variables • 351, 357

version numbers • 47, 49

version numbers, for policies • 47, 49

W

Web activity • 43

X

x-headers • 168, 170

x-headers, detecting • 307, 309