CA DataMinder

Administration Guide

Release 14.5

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 may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, 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 © 2013 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.

Contents

Chapter 1: About the Administration Console 13

Administration Console Overview....14
Console Screens....14
User Administration....15
Machine Administration....16
Logfiles....18
Searches Screen....18
Find Items....23

Chapter 2: Tools 25

Administration Search....25
Install a Full License File....26
Install System Definition File....26
Binary Text Extractor Configuration File....27
US Social Security High Group File....28
Client Network Agent Configuration File....28
Set Password for the Database Primary User....30
Set Credentials for the Reporting User....30
Configure the Data Warehouse....32
Manage Policy Classes....33
Manage Security Models....33
Manage Policy Roles....35
Manage User Roles....35
Manage System Files....36
Account Import Overview....37
Replicate CMS Changes to Clients....37
Generate Checkpoints....38
Audit Options....39
Console Options....40
Define a Dynamic Address List....41

Chapter 3: Administration Searches 43

Overview....43
Predefined Administration Searches....44
Run an Existing Administration Search....45
Run a New Administration Search....46

Wildcards 48
Backslashes 49
Searching by User Name 50
Searching by User Group 50
SQL Search Expressions 51
Saved Searches - Administration Data 53
Search Results: Available Actions 54

Chapter 4: CMS Administration 57

Multiple CMSs 57
CMS Groups 58
Connect to a CMS 58
Enable Single Sign-on 60
Security Models 60
Manage Security Models 62
Policy Security Models Not Compatible With Some Reports or Review Queue 64
Suspend or Resume a Machine 64
Backing Up and Restoring the CMS 65
Overview 65
General Backup Tasks 66
Backup Tasks for SQL Server 66
Backup Tasks for Oracle 67
Restoring the CMS 68
Manage System Files 69
View System Files 69
Edit System Files 70
Replace System Files 71

Chapter 5: Content Registration 73

About Content Registration (Fingerprinting) 73
Fingerprinting Components 74
Content Agent Types 75
Plain Text Embedded File Agents Are Superseded 76
Using Content Agents to Detect Printed Files 77
Using Content Agents to Detect Spreadsheets 78
How to Set Up Content Agents 79
To create a content agent 79
To add files that you want to protect 82
Build a Content Index 82
To publish a content index 83
Set up Content Agent Triggers 84

Chapter 6: Data At Rest Scans 85

Data At Rest Scans....85
Manage Scanning Jobs....86
Create a Scanning Job....88
Scheduled Scanning Jobs....89
Database Scanning Jobs....90
Command Line Scanning Jobs....91
Import Version 6.0 Scanning Jobs....92
Purge the Scan Database....92
    Scanned File Database....93
Binary Data Handling....93
    Store Binary Data as Event Attachments = True....94
    Store Binary Data as Event Attachments = False....95
Specify FSA Server Properties....96
FSA User Accounts....97
    FSA Run As User....98

Chapter 7: Event Auditing Setup 101

Overview....101
Audit Options....102
    Set up Audit Field Labels....103
    Populate Audit Field Lists....104
    Set up the iConsole Audit Buttons....107
    Set up Audit E-mail Templates....108
Suppress Automatic Auditing....109
About the Review Queue....109

Chapter 8: Logfiles 111

Overview....111
Log Types....113
    About Policy Incident Logs....115
Find Log Entries....116
View Log Files....117
Configure Log Files....118
Write to Windows Event Log....119
Write to a Syslog Server....121

Chapter 9: Machine Administration 123

Overview....124

Machine Types 125
Managing Machine Accounts 125
Add New Machines 126
Move Machines 127
Delete Machines 127
Rename Machines 128
Export the Machine Hierarchy 128
Import or Reparent Machines 129
Replication 129
Replicate CMS Changes to Client Machines 130
Replicate Captured Data to Parent Servers 130
Replication Notification Periods 131
Disable Replication 132
Replication Over Slow Network Connections 133
Replication Failures 133
Infrastructure 133
Overview 134
Stop or Restart the Infrastructure without Rebooting 134
Run the Infrastructure as a Named User 135
Editing Machine Policies 135
File Scans 135
Disabling E-mail and Browser Integration - Machine Administration 136
Monitoring Free Disk Space 137
Monitoring Free Disk Space Overview 138
Disk Space Policy Settings 139
Suspended Machines 139
Overview 140
What Operations are Still Available on Suspended Machines? 141
Suspend or Resume a Machine 142
Data Encryption 142
Encrypt Replicated Data 142
Encrypt Stored Data 143
Data Compression 146
Event Purging 146
Overview 147
Purging Strategies 148
What Data is Purged? 149
Minimum Retention Period 150
Purge SPs 151
Configure Purges in the Machine Policy 152
Selective Trigger-Based Purging 153
Turn off Purging 154

Purge Policy Settings 155
Diagnostics 156
Overview 157
Configure Diagnostics Collection 158
Replication Checkpoints 160
Configure Checkpoints 162
Diagnosing Missed Checkpoints 163

Chapter 10: Machine Policy Settings 163

Edit a Policy 164
Edit Common Machine Policies 164
Policy Navigation 165
What Is in a Machine Policy? 165
Infrastructure Settings 166
Policy Engine Settings 178
Client File System Agent Settings 180
Client Network Agent 187
Central Management Server Settings 188

Chapter 11: Mapping E-mail Addresses to Users 189

Overview 189
Which Features use Address Mapping? 190

Chapter 12: User Administration 193

Administrators 193
Administrator Responsibilities 194
User Accounts 195
New user Accounts 196
Delete Users and Groups 198
Recreate Users 198
User Groups 199
Default Group 200
Set the Default Group 201
Add New Groups 201
Move Users Between Groups 202
Rename Users or Groups 203
Export the user Hierarchy 203
User Properties 204
Privileges 205
Passwords 211

Security Models 211
Policy Roles 218
User Roles 220
Management Groups 226
Addresses 227
Attributes 228
Exempt Users 228
Manually Exempt Users From Policy 229
Account Import 230
Account Import Overview 231
Synchronize E-mail Addresses 231
Import Methods and Sources 232
Handling for Unknown Users 233
Multiple attribute Values 234
Modify LDAP Values with Conversion Expressions 234
Automatically Exempt Users From Policy 235
Account Import Log Files 235

Chapter 13: User Policies 237

What is in a User Policy? 238
Policy Versions 238
Policy Version Numbers 239
Policy Version Example 239
Reported and Assigned Policy Versions 241
User Policy Editor 242
Policy Navigation 243
Policy Reports 244
Edit a Policy 246
Find a Policy Folder or Setting 246
Export, Import, and Copy Policies 247

Chapter 14: Troubleshooting 249

General Troubleshooting 249
Can I Rename Users? 250
Can I Rename CA DataMinder Computers? 252
Cannot Connect to CMS Because Database Password Has Changed 252
Clients and Gateways Cannot Connect to CMS 253
Passwords Are Exposed in the Data Management Console 254
Data Replication Suddenly Stops When Using ADSL 255
E-mail Troubleshooting 255
CA DataMinder Captures an Email or Attachment With a Virus 256

Delays When Sending Emails to Many Recipients or Large Distribution Lists 256
I Cannot Forward Emails That Have Been Redirected 257
Integration With Outlook Stops Working 258
Address Lookup Commands Fail if User Display Name is Changed 260

Appendix A: Accessibility Features 261

Display 261
Sound 262
Keyboard 262
Mouse 263

Index 265

Chapter 1: About the Administration Console

Use the CA DataMinder Administration console to manage user and machine accounts, edit policies, create content agents, run administration searches, and manage scanning jobs.

This section contains the following topics:

Administration Console Overview (see page 14)
Console Screens (see page 14)
Find Items (see page 23)

Administration Console Overview

The Administration console includes the following components:

User Administration

Lets you manage user accounts and organize users into groups.

User Policy Editor

Lets you edit policies for user groups or individual users. These policies govern how users use e-mail, print, manage files, and access the Web.

Machine Administration

Lets you manage CA DataMinder computers; CMSs, gateways and client machines.

Machine Policy Editor

Lets you edit policies for CA DataMinder machines. These policies govern how these machines manage their local databases and how they exchange data with other CA DataMinder machines.

Logfiles

Displays logfiles of all significant replication and activity events. These include when users and machines log in or out, and when policies are created or edited locally.

Searches

Lets you run administration searches for user and machine accounts. These include 'information' and 'health' searches. Information searches retrieve basic account details; health searches identify problematic accounts, or accounts which require your attention.

File Scanning Agent (FSA)

Lets you scan and analyze data and apply appropriate controls. The FSA can scan the text content of files, items in Exchange Public Folders, and items on SharePoint sites.

More information:

User Administration (see page 15)
Machine Administration (see page 16)
Logfiles (see page 18)
User Policy Editor (see page 15)
Machine Policy Editor (see page 17)

Console Screens

More information:

User Administration (see page 15)
Machine Administration (see page 16)
Logfiles (see page 18)
Searches Screen (see page 18)

User Administration

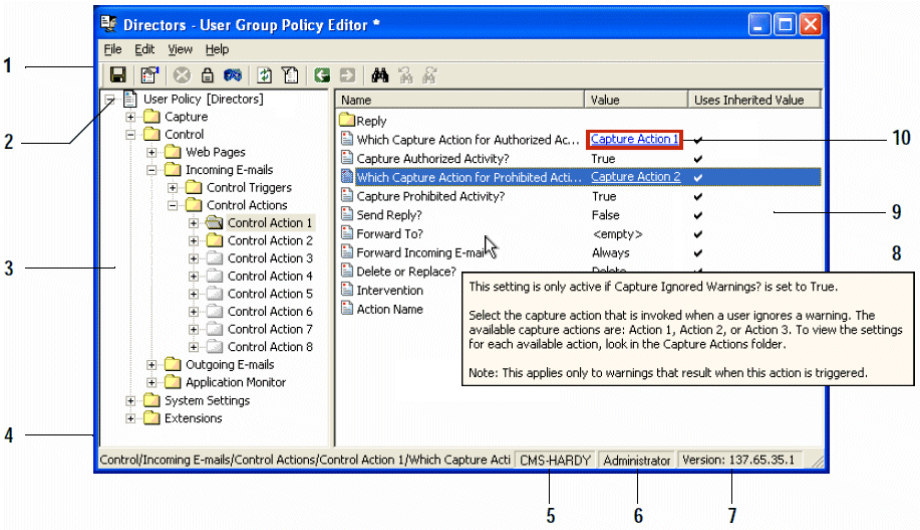
The User Administration screen is where you manage user accounts and user groups. You can organize users into hierarchical groups, assign administrative privileges, and set passwords for individual users. You can also launch the User Policy Editor directly from this screen.

More information:

Reported and Assigned Policy Versions (see page 241)

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:

Policy Version Numbers (see page 239)
Policy Navigation (see page 165)

Machine Administration

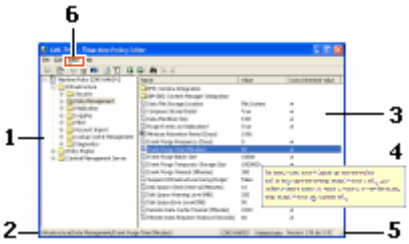
The Machine Administration screen is where you manage accounts for the Central Management Server (CMS) and your gateway and client machines. You use this screen to manage machine accounts and view the current status of each CA DataMinder machine. You can also launch the Machine Policy screen directly from this screen.

More information:

Machine Policy Settings (see page 163)

Machine Policy Editor

The Machine Policy Editor is where you edit policies for the CMS, gateways, and client machines. These policies govern how CA DataMinder machines manage their databases and how they exchange data with other CA DataMinder machines.



1. **Policy folders pane**

   Shows all the folders available for viewing or editing in the current policy. Icon variations show the folder status (disabled, enforced, or hidden). You can also double-click a folder to view or edit its attributes.

2. **Path bar**

   Shows the location of the current folder or setting within the policy.

3. **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.

   Policy explanations

4. Roll your mouse over any folder or setting to see a pop-up explanation. Help is also available when you double-click a policy item.

5. **Policy version**

   Shows the current policy version number. This enables administrators to track local and inherited policy updates.

6. **Automatically Enforce Modified Settings**

   Find this setting in the Tools menu. It affects parent-child inheritance for policies. By default, this setting is not selected.

   If you do select this setting, any change made in a common gateway policy or common client policy is automatically applied and enforced in all gateway policies or client policies respectively.

More information:

Machine Policy Settings (see page 163)
Policy Version Numbers (see page 239)

Logfiles

The Logfiles screen displays logfiles of all significant system events. For example:

- Activity logfiles record when users and machines log in or out, and each time policies are created or updated using a Policy Editor running on the local machine.

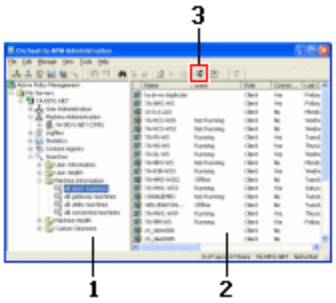
  For example, if an administrator edits a user's policy using an Administration Console on a remote machine, the edit session is recorded in a log file on the remote machine.
- Replication logfiles record any database changes that were made on a remote machine and copied to the local machine, for example, policy updates.
- System logfiles record any infrastructure errors that occur while the CA DataMinder service is running.
- Account Import logfiles record the outcome of any operations using the User Import wizard.

More information:

View Log Files (see page 117)

Searches Screen

The Searches screen is where you run administration searches for users or machines. For example, you can search for user accounts with out-of-date policies or machines that have missed one or more replication checkpoints.



1. Available searches

   Lists all predefined user and machine searches, plus any custom searches saved on the current machine. Click the search you want; the search runs automatically. Searches are organized into the following folders:

   User Information

   These focus on user accounts that are active or currently logged in, or which have had policy changes since the account was created.

   User Health

   These focus on accounts that require your attention, such as uses with out-of-date policies or unused accounts.

   Machine Information

   These identify existing client machines, gateways and utility machines, plus machines currently connected to the CMS.

   Machine Health

   These diagnostic searches focus on machines that require your attention, such as suspended machines or machines that cannot be contacted, machines with out-of-date policies or CA DataMinder software, and machines with a replication backlog or which have failed to acknowledge recent checkpoints.

   Custom Searches

   If you define and save your own administration searches, they are listed here.

   Note: To cancel a search (for example, because if it is taking too long), right-click the search and click the Stop Search button.

2. Results

   Lists the users, groups or machines matching the search criteria. See Administration search results.

   Right-click any object and choose an available action.

3. Administration Search button

   Click the Administration Search button to define a new custom search.

More information:

Overview (see page 43)
Administration Search Results (see page 20)
Search Results: Available Actions (see page 54)

Administration Search Results

For predefined administration searches, the following details are included in the search results screen:

User Searches

Data returned by these searches can include:

Assigned Policy Version

The version of the latest policy assigned to a user or group. This version is held on the CMS and replicated automatically to the relevant gateway or client machine at intervals determined in the CMS policy.

Base Group

The management group or subgroup to which the user belongs.

Creation Time

Date and time when the account was created.

Fullname

The user's display name that appears in the iConsole and Data Management console.

Last Login Time

The date and time when the user last logged into CA DataMinder.

Machine

The computer being used by users currently logged into CA DataMinder.

Name or UserName

The CA DataMinder logon name for the user.

Native User

The Windows logon account for users currently logged into CA DataMinder.

Reported Policy Version

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

Role

The role assigned to the current user. This role determines the default set of privileges assigned to that user.

Machine Searches

Data returned by these searches can include:

Assigned Policy Version

The version of the latest policy assigned to a machine. This version is held on the CMS and replicated automatically to the relevant gateway or client machine at intervals determined in the CMS policy.

Checkpoint Reply Time (minutes)

The average time that the machine takes to send a checkpoint acknowledgment. Use this data to identify machines that are slow to respond. Such information can help identify replication latencies on your network.

Children

The number of child machines parented to the current server.

Connected Y/N

Identifies machines currently logged into CA DataMinder.

Created

The date and time when the machine account was created.

Days Since Checkpoint Reply

The number of days since the machine last sent a checkpoint acknowledgment.

Note: More accurately, this count shows the number of full 24 hour periods since the last acknowledgment.

Downstream Queue

The number of infrastructure changes (policy and hierarchy objects) that the current machine has not yet received from its parent server.

Last Connection

The date and time of the most recent connection when the machine was last connected.

Last Replication Time

The date and time when infrastructure updates were last received from the parent server.

Name

The name of the CA DataMinder machine.

Parent

The name of the parent server.

Reported Policy Version

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

Role

Client, Gateway, Utility or CMS.

Software Version

The version of CA DataMinder running on this machine.

State

This column shows OK or an error code.

The error code indicates the cause of the current machine state. For example, the error code for a suspended machine may indicate the cause of the suspension.

Status

The current operational status of the machine. Possible values are Running, Offline, Stopped or Failed.

Note: Failed means that the CA DataMinder infrastructure failed to start.

Synchronization State

Indicates whether the CA DataMinder infrastructure on the current machine is fully with its parent server.

Unanswered Checkpoints

The number of checkpoints that have not been acknowledged by the current machine.

Upstream Queue

The number of outstanding objects (captured or imported events) awaiting replication up to the parent server.

More information:

Overview (see page 43)
Search Results: Available Actions (see page 54)

Find Items

Use the Find feature to quickly find items such as computers, user groups, or administrative searches.

To find items

1. Click or press Ctrl+F.
2. Enter the item name in the Find Items 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.
3. Specify whether to search up or down from your current location in the left-hand pane.
4. You can quickly find other occurrences of this name. To find:

   - The previous occurrence of this name, click or press Shift+F3.
   - The next occurrence of this name, click or press F3.

   Note: Find can only find items that are currently visible, or that were recently visible. That is, it can look for items in branches that are currently expanded, or that were previously expanded but are now collapsed. It cannot find items in branches that have never been expanded (in the current session). See the examples below.

Chapter 2: Tools

This section contains the following topics:

Administration Search (see page 25)
Install a Full License File (see page 26)
Install System Definition File (see page 26)
Set Password for the Database Primary User (see page 30)
Set Credentials for the Reporting User (see page 30)
Configure the Data Warehouse (see page 32)
Manage Policy Classes (see page 33)
Manage Security Models (see page 33)
Manage Policy Roles (see page 35)
Manage User Roles (see page 35)
Manage System Files (see page 36)
Account Import Overview (see page 37)
Replicate CMS Changes to Clients (see page 37)
Generate Checkpoints (see page 38)
Audit Options (see page 39)
Console Options (see page 40)

Administration Search

Administration searches let you search for user, group and machine accounts. For example, you can search for user accounts with out-of-date policies or machines that have missed one or more replication checkpoints.

A range of predefined searches are available in the Administration console. These include 'information' and 'health' searches, for both users and machines. Information searches typically retrieve basic details about existing accounts; health searches identify problematic accounts, or accounts which require your attention, such as machines which cannot be contacted or users with out-of-date policies.

You can also define and save your own administration searches, and copy search results to the clipboard. In all cases, CA DataMinder generates a SQL search expression. If required, experienced users can edit this expression directly.

Note: For help on event searches, see the Data Management console or iConsole online help.

More information:

Run an Existing Administration Search (see page 45)
Run a New Administration Search (see page 46)
Saved Searches - Administration Data (see page 53)
Search Results: Available Actions (see page 54)

Install a Full License File

Although the Tools menu in the Administration console includes an option to install a license file, you do not need to install a license file to be able to use and deploy CA DataMinder.

In the future, CA Technologies may provide you with a license file that unlocks new features. You only need to install a license file if instructed to do so by CA Technologies technical staff.

Install System Definition File

CA DataMinder system files include such items as definition files for US social security numbers, configuration files for the Binary Text Extractor and Client Network Agent, dynamic address lists and audit mail templates. CA DataMinder stores these system files in the CMS database.

The Administration console includes the System File Explorer for managing system files. The System File Explorer is very similar to Windows Explorer and displays the internal file system within the CMS database. It lets you browse the internal file system to view, edit, and replace system files.

To install a system definition file

1. Log on to the Administration console using an account that has the 'Admin: Manage System Files' administrative privilege.
2. Click Tools, Install System Definition File.

   The Install System Definition File dialog appears.
3. Click the system file that you want in the File Type list.

More information:

Binary Text Extractor Configuration File (see page 27)
US Social Security High Group File (see page 28)
Client Network Agent Configuration File (see page 28)
Manage System Files (see page 36)

Binary Text Extractor Configuration File

The Binary Text Extractor (BTE) is a configurable utility that can extract the text content from document types that are not normally supported by CA DataMinder. Policy engines and endpoint agents can then apply CA DataMinder policy to these files as normal.

For example, if you need to analyze information stored in proprietary or industry file formats, or even in executable files, you can configure the BTE to extract the text content from these file types.

Configuration details for the BTE are saved in BinaryTextorConfig.xml. This is a CA DataMinder system definition file. To configure BinaryTextorConfig.xml, follow these steps:

1. Export the default version of BinaryTextorConfig.xml from the CMS.
2. Edit BinaryTextorConfig.xml to specify the file types that you want CA DataMinder to analyze.
3. Install your customized version of BinaryTextorConfig.xml back onto the CMS.

   CA DataMinder then replicates your customized version of BinaryTextorConfig.xml automatically to each CA DataMinder policy engine and endpoint computer.

For details about exporting and editing BinaryTextorConfig.xml, see the Binary Text Extractor chapter in the CA DataMinder *Platform Deployment Guide*.

To install a customized BinaryTextorConfig.xml

1. Log on to the Administration console using an account that has the 'Admin: Manage System Files' administrative privilege.
2. Click Tools, Install System Definition File.

   The Install System Definition File dialog appears.
3. Click 'Binary Text Extractor Configuration File' in the File Type list.
4. Browse to the BinaryTextorConfig.xml file that you edited.
5. Return to the Install System Definition File dialog and click Install.

   CA DataMinder automatically replicates BinaryTextorConfig.xml to all policy engines and endpoint computers.

US Social Security High Group File

To detect social security numbers using the %SSN% variable, CA DataMinder needs to refer to a specific system definition file. That is, the US Social Security High Group File. A version of this file is provided with CA DataMinder, but to ensure the data remains accurate, we recommend that you update the file regularly (for example, on a monthly basis).

Note: 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.

To install the system definition file

1. Browse to the following Web site:

   `www.socialsecurity.gov/employer/ssnvhighgroup.htm`

2. Right-click the US Social Security High Group File that you want and choose Save Target As to save the information as a .txt file on your local computer.
3. Log on to the Administration console using an account that has the 'Admin: Manage System Files' administrative privilege.
4. Click Tools, Install System Definition File.

   The Install System Definition File dialog appears.

5. Click US Social Security High Group File in the File Type list.
6. Browse to where you saved the text file.
7. Return to the Install System Definition File dialog and click Install.

   The file is installed to the CMS where it can be referenced for %SSN% confirmation.

Client Network Agent Configuration File

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.

However, certain web sites require special handling by the network agent. Site-specific handling instructions for these sites are implemented in the Client Network Agent configuration file. For example, this configuration file includes instructions to ensure that Outlook.com continues to operate correctly after the network agent blocks a web mail.

The default configuration file contains handling instructions for several popular web sites. It is installed automatically when you deploy the network agent.

However, we may release occasional updates if we discover additional sites that require special handling. Also, you may need to install a custom configuration file if your organization requires custom handling for a specific web site. If CA technical staff instruct you to deploy an updated or custom configuration file, use the Administration console to install the file onto your CMS.

Important! Install new Client Network Agent configuration files only if instructed to do so by CA technical staff!

To install a CNA configuration file

1. Log on to the Administration console using an account that has the 'Admin: Manage System Files' administrative privilege.
2. Click Tools, Install System Definition File.

   The Install System Definition File dialog appears.
3. Click 'Client Network Agent Configuration File' or 'Client Network Agent Configuration File (Custom)' in the File Type list.
4. Browse to the configuration file.

   The files are named CNAConfig.xml or CNAConfig_custom.xml respectively.
5. Return to the Install System Definition File dialog and click Install.

   CA DataMinder automatically replicates the configuration file to all endpoint computers hosting the network agent.

For details about the Client Network Agent, see the *Endpoint Integration Guide*.

Set Password for the Database Primary User

You can change the password for the Primary User database account. This is the main CA DataMinder database account. The infrastructure uses this account to access the CMS database. For further details, see the *Database Guide*; search for 'primary user'.

If the password has been changed on the database server (for example, for security reasons), you must supply CA DataMinder with the new password. You can do this directly from the Administration console.

Follow these steps:

1. Log on to the Administration console using an account that has the 'Admin: Manage security models' privilege.
2. Click Tools, Set Database Primary User Password.
3. Enter the new password in the Set Database Primary User Password dialog.

More information:

Privileges (see page 205)

Set Credentials for the Reporting User

You must specify a Reporting User database account if you enable data warehousing. External reporting applications (such as BusinessObjects Enterprise) use this database account to connect to the Data Warehouse and CMS database.

You can use the Administration console to add or modify credentials for the Reporting User database account. For example, if the password has been changed on the database server (for example, for security reasons), you can supply CA DataMinder with the new password.

To set credentials for the Reporting User

1. Log on to the Administration console using an account that has the 'Admin: Manage security models' privilege.
2. Click Tools, Set Reporting User Credentials.
3. Enter the user name and password in the Set Reporting User Credentials dialog.
4. (Optional) If necessary, provide credentials for an existing Database Administrator account. See below for details.

   For Oracle CMS databases, this Database Administrator account *must* have the following system privileges:

   ```
   CREATE SESSION
   RESOURCE
   DBA
   SYSDBA
   ```

When must I provide Database Administrator details?

Credentials for the Reporting User are securely stored in the CMS database and in the CMS internal file system. The two sets of credentials must be in sync.

You do *not* need to provide Database Administrator details if a DBA has already updated the Reporting User credentials in the CMS database. In this situation, CA DataMinder only needs to update the Reporting User credentials stored in the CMS internal file system.

You *do* need to provide Database Administrator details if the CMS database has not been updated yet. In this situation, CA DataMinder simultaneously adds the Reporting User credentials to the CMS internal file system and the CMS database. CA DataMinder uses the Database Administrator account to log in to SQL Server or Oracle and update the CMS database.

More information:

Configure the Data Warehouse (see page 32)

Configure the Data Warehouse

The Data Warehouse is a set of database tables containing CA DataMinder event data that has been transformed into a format suitable for generating reports and iConsole dashboards.

The Data Warehouse is installed automatically when you install a new CA DataMinder CMS, but you must explicitly enable the data warehouse if you want to use the iConsole dashboard or run BusinessObjects reports for CA DataMinder.

You can also reconfigure the Data Warehouse if it is already enabled. For example, you may want to change the settings for off-peak processing jobs or data purges.

To configure the Data Warehouse

1. Log on to the Administration console using an account that has the 'Admin: Manage security models' privilege.
2. Click Tools, Configure Data Warehouse.
3. Configure the following settings:

   General Options

   These settings enable or disable the Data Warehouse. They also specify which data gets copied into the Data Warehouse. In particular, they specify whether to include event participant data. Other settings enable regular purges of older data from the Data Warehouse.

   Important! You must collect event participant data if you intend to run BusinessObjects reports..

   Additional Population and Maintenance

   These settings configure off-peak processing jobs for the Data Warehouse.

   Advanced Options

   These settings configure batch sizes for data warehousing jobs. Other settings enable you to resynchronize the Data Warehouse with data in the CMS database or to purge and repopulate the entire Data Warehouse.

Note: For further details, see the *Platform Deployment Guide*; search for 'data warehouse'.

More information:

Set Credentials for the Reporting User (see page 30)

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.

Manage Security Models

Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database for events.

CA DataMinder supports multiple security models, including models based on management groups, variants of this original model (for example, to prevent reviewers reviewing their own e-mails), and policy-based models. You can choose which models are active on your CMS and multiple models can be active at the same time. However, each reviewer can only be linked to a single model. For example, some reviewers may only be permitted to see events linked to users in their own management group. Other reviewers may only be to see specific types or categories of events.

When you first install CA DataMinder, only one security model is active. This is the default security model, Management Group (Standard). You must enable other security models before you can assign them to reviewers.

You can manage security models in the Administration console.

To enable a security model on the CMS

1. Choose Tools, Manage Security Models.
2. In the Manage Security Models dialog, click Add.
3. In the Create Security Model dialog, you can configure the model you want. You need to:
   - Set the database user name. You must provide the name and password for a secure database account.

     CA DataMinder consoles use these credentials to connect to the CMS database when searching for events under the new security model.

     Important! Each security model must use its own database account. Security models cannot share the same database account.
   - Set the model type. You must choose from the available types, such Management Group (Sender).

     If required, you can add a hybrid security model. This combines two security models to filter the results when a reviewer searches for events.

To modify a security model

1. Choose Tools, Manage Security Models.
2. Select model you want and click Modify.

   You can now change the database user name or model type.

To remove a security model

1. Choose Tools, Manage Security Models.
2. Select model you want and click Remove.

   Any reviewers still assigned to this model will revert to the default security model. (Typically, this is the Management Group (Standard) model, although you can change the default model type.)

More information:

Security Models (see page 60)

Manage Policy Roles

Each policy role is associated with a set of specific policy classes and individual policies. You can define as many policy roles as you need.

To add a role

1. In the Administration console, click Tools, Manage Policy Roles.
2. In the Manage Policy Roles dialog, click Add to define a new policy role.

To modify a role

1. In the Administration console, click Tools, Manage Policy Roles.
2. Select a policy role and click Modify.
3. In the Policy Role dialog, choose the policy classes or individual policies that you want to associate with the policy role.

To remove a role

1. In the Administration console, click Tools, Manage Policy Roles.
2. Select a policy role and click Remove.

Important! If you remove a policy role while users are still assigned to it, these users will have no policy role. Consequently, they will be unable to view **any** events in the iConsole until you reassign a policy role to them!

Manage User Roles

Each user in CA DataMinder is assigned to a user role, for example, Administrator, Manager, or User. The user role determines the default set of administrative privileges assigned to the user and their security model.

You can redefine, rename and create user roles if you have the Admin: Edit user roles privilege.

If you change the default set of privileges assigned to a user role, CA DataMinder automatically updates the privileges of all users in that role. For example, if you add a privilege to the Manager role, all users in the Manager role are automatically granted the new privilege.

Note: If future versions of CA DataMinder introduce new privileges to a default role, these privileges are granted automatically to all users assigned to that role when you upgrade CA DataMinder.

To redefine a role

1. Click Tools, Manage User Roles.
2. In the Manage User Roles dialog, select the role that you want to edit.
3. If required, you can:
   - Rename the role.
   - Assign or remove administrative privileges.
   - Set the default security model.
   - Set the default policy model.

To create a new role

1. Click Tools, Manage User Roles.
2. Click New to display the Create New User Role dialog.
   a. Enter a name for the new role.
   b. Specify which existing role you want to copy from.

      The administrative privileges assigned to the existing role are copied to the new role.
   c. Click OK to close the dialog.

      The new user role is created.
3. If required, modify the administrative privileges and default security model assigned to the new role.

Manage System Files

If a problem occurs with your CA DataMinder installation, you may be instructed to examine system files stored in the CMS database. Analysis of the system files can often help CA technical staff diagnose the problem.

CA DataMinder system files include such items as iConsole search definitions, content registration agents, definition files for social security numbers, dynamic address lists and audit mail templates. CA DataMinder stores these system files in the CMS database. Each system file has two parts: the file metadata and the actual file content. The metadata includes such details as the file name and creation date. The file content itself comprises XML or binary data.

The Administration console includes the System File Explorer for managing system files. The System File Explorer is very similar to Windows Explorer and displays the internal file system within the CMS database. It lets you browse the internal file system to view, edit, and replace system files.

More information:

View System Files (see page 69)
Edit System Files (see page 70)
Replace System Files (see page 71)

Account Import Overview

To simplify mass deployments, you can use the Account Import feature to import user details into CA DataMinder from an external Lightweight Directory Access Protocol (LDAP) directory or a source file. Account Import can:

- Import new users and groups into the existing CA DataMinder user hierarchy.
- Reorganize existing CA DataMinder users to synchronize them with an external user hierarchy, for example, an LDAP directory structure.
- Create new CA DataMinder accounts for unknown users. These are imported users who have no corresponding account in CA DataMinder.
- Add a domain as a prefix to all imported user account names, such as unipraxis\frankschaeffer.
- Update CA DataMinder user accounts with imported attributes such as e-mail addresses and employee IDs.
- Exempt specific users from policy. CA DataMinder can exempt users with specific LDAP Attributes or, if you import from an XML data file, users with the *policyexempt* attribute.

Note: For full details about user import operations, see the *Platform Deployment Guide*; search for 'Account Import'.

Replicate CMS Changes to Clients

The CMS database holds policy details for each CA DataMinder user and machine, and administration details for each user, user group and machine. Any database changes are replicated automatically to child machines. The replication frequency is determined by the CMS machine policy. But you can request immediate replication. This is useful where CA DataMinder runs on networks using a slow CMS-to-child replication interval. To do this, choose Tools, Replicate changes to clients.

Note: You can also request warnings before you replicate changes. Choose Tools, Options and go to the General tab. Then, when you next replicate changes, CA DataMinder asks you to confirm the replication.

More information:

Replicate Captured Data to Parent Servers (see page 130)
Replication Notification Periods (see page 131)
Disable Replication (see page 132)

Generate Checkpoints

(Optional) You can manually generate checkpoints. For example, you can send a custom checkpoint after making changes to your user hierarchy or after running a major Account Import job.

To set a manual checkpoint

1. Choose Tools, Generate Checkpoint.

   The Generate Checkpoint dialog appears.

2. Enter a description of the checkpoint and click Generate.

   A checkpoint ID appears in the dialog. You can copy the checkpoint ID to the Windows clipboard for use when running a custom administration search for machines.

   Note: The description, along with the checkpoint ID, is stored in the Wgn3Checkpoint database table.

3. Close the dialog.

Audit Options

For reviewers to make full use of the iConsole event audit features, administrators need to configure the following features in the Administration console:

Audit fields

Field labels and list items in the iConsole Issue dialog are fully configurable, so that the terminology used and the available options can be customized to meet your organization's requirements. For example, administrators can define multiple 'audit status' labels, 'actions taken' labels and other predefined comments. They can also specify additional, mandatory updates to the audit trail when a reviewer changes an event's audit status. For audit e-mails, administrators can also predefine recipient addresses and the e-mail subject.

Audit buttons

Administrators can customize the behavior of audit buttons in the iConsole toolbar. These buttons allow reviewers to instantly change specific audit details from one value to another. For example, they can configure a button to automatically change the audit status of the currently selected events, or to change the 'Action Taken' from 'Reviewed' to 'Referred to Compliance Officer'. Up to five separate buttons can be configured.

Note: If an administrator reconfigures the iConsole audit buttons, these changes will only become effective the next time a user logs into the iConsole. Users currently logged on to the iConsole must log off and log back on before these changes become effective.

Audit e-mail templates

Administrators can define templates for audit e-mails and make them available to reviewers in the iConsole (in the Compose Email dialog). These templates can include predefined recipient lists, plus predefined body and subject text to match your organization's terminology and requirements. Reviewers can use these templates, and change the predefined details if necessary, when composing audit e-mails.

Important! If these event auditing features are not fully configured in the Administration console, then event auditing will not be available in the iConsole. That is, reviewers will not be able to audit events in either console.

More information:

Set up Audit Field Labels (see page 103)
Populate Audit Field Lists (see page 104)
Set up Audit E-mail Templates (see page 108)

Console Options

You can customize the behavior of certain console features.

1. Choose Tools, Options.
2. In the Options dialog, click the tab you want:

General tab

Use this tab to set warning options in the Administration console.

User Attributes tab

Use this tab to define customized user attributes. For example, you can create an Employee ID attribute and assign a unique ID to each user in your organization.

Address Lists tab

Use this tab to define dynamic address lists. A dynamic address list is an SQL query designed to generate a list of e-mail addresses. See the following section for details.

Content Proxy tab

Use this tab to connect an iConsole or Data Management console to a content proxy server. You must specify a content proxy server in order to run content searches.

File Scanning Agent tab

Use this tab to optionally set a refresh interval for File Scanning Agent scanning jobs. Any changes in a job's status are shown when the job list refreshes.

Content Registration tab

Use this tab to configure warnings and refresh intervals for content agents.

Note: Press Ctrl+Tab to switch between tabs.

Define a Dynamic Address List

CA DataMinder lets you define dynamic address lists. A dynamic address list is an SQL query designed to generate a list of e-mail addresses. These address lists are available to users sending e-mails from the iConsole. They are primarily used to generate lists of recipients when an administrator sends an e-mail notification.

To define a dynamic address list

1. Choose Tools, Options and select the Address Lists tab.
2. To define a new list, click Add.
3. To modify an existing address list, double-click a list or select a list and click Modify.
4. In the resulting Address List dialog, provide a name for the address list and add the SQL query to retrieve the users you want.

Chapter 3: Administration Searches

This section contains the following topics:

Overview (see page 43)
Predefined Administration Searches (see page 44)
Run an Existing Administration Search (see page 45)
Run a New Administration Search (see page 46)
Saved Searches - Administration Data (see page 53)
Search Results: Available Actions (see page 54)

Overview

Administration searches let you search for user, group and machine accounts. For example, you can search for user accounts with out-of-date policies or machines that have missed one or more replication checkpoints.

A range of predefined searches are available in the Administration console. These include 'information' and 'health' searches, for both users and machines. Information searches typically retrieve basic details about existing accounts; health searches identify problematic accounts, or accounts which require your attention, such as machines which cannot be contacted or users with out-of-date policies.

You can also define and save your own administration searches, and copy search results to the clipboard. In all cases, CA DataMinder generates a SQL search expression. If required, experienced users can edit this expression directly.

Note: For help on event searches, see the Data Management console or iConsole online help.

Predefined Administration Searches

The Searches screen in the Administration console includes a wide range of predefined searches:

User Information

These focus on:

- User accounts that are active or currently logged in
- User accounts whose policy has been modified since the account was created.
- User accounts that are exempt from policy. *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.

User Health

These searches focus on:

- User accounts with out-of-date policies. That is, the child machine is not using the latest policy version held on the CMS. Specifically, the reported policy does not match the assigned policy.
- Unused user accounts. These are accounts that exist on the CMS but which have never logged on.
- User accounts with no parent group, and user or group policies with no parent policy. Both situations can potentially arise if the user hierarchy becomes corrupted in the CMS database.

Machine Information

These searches identify current machine accounts (separate searches are available for each machine type) and machines currently connected to the CMS.

Machine Health

A wide range of diagnostic searches are available. For example, you can search for:

- Suspended machines, machines that cannot be contacted, or CA DataMinder machines on which the infrastructure has stopped.
- Machines that need a complete infrastructure synchronization with their parent server.
- Machines running the latest version of CA DataMinder, or machines running an out-of-date version.
- Machines that have missed one or more replication checkpoints.
- Machines with a replication backlog—either infrastructure updates waiting to be sent down to child machines, or captured events waiting to be sent up to the parent server.

More information:

Administration Searches (see page 43)

Run an Existing Administration Search

To run an existing administration search

1. Log on to the Administration console using an account that has the 'Admin: Allow administration searches' administrative privilege.
2. Expand the Searches branch and click the search you want.

   The search runs automatically.

   If you need to cancel the search (for example, because if it taking a long time to complete), click the Stop Search button.
3. When the search completes, all matching user or machine accounts are listed in the right-hand pane.

   For user searches only, you can double-click any user listed in the right-hand pane to view their full account properties.

More information:

Administration Searches (see page 43)

Run a New Administration Search

To define a new administration search

1. Log on to the Administration console using an account that has the 'Admin: Allow administration searches' administrative privilege.
2. To create a new administration search, choose Tools, Administration Search.

   To edit an existing search, expand the Searches branch in the left-hand pane. Right-click the search you want and choose Edit.
3. Fill in the fields in the Administration Search dialog:

   CMS

   If your Console is linked to multiple CMSs, choose the CMS whose database you want to search.

   Look For

   Choose which items you want to look for: Machines, User Groups or Users.

   View

   (Only available for machine searches) The view determines which data is returned by a database query. In effect, it determines which columns are shown in the right-hand pane. Choose a Generic or Diagnostics view:

   - Use a Generic View to return basic machine details. These include the machine role (for example, a client machine or gateway), its policy versions, its parent server, the number of children (child machines parented to the current server) and the CA DataMinder software version.
   - Use a Diagnostics View to include various status columns, in addition to the usual machine details. For example, these details indicate the connection status, replication status (including missed checkpoints), and whether a machine needs resynchronizing. You use this data to identify machines that which require your attention.

   Filters

   Define your search using the available search filters. These are shown on tabs below. For example, if looking for users you can search by user group or last logon date.

   Note: All search fields that require text input support automatic and manual wildcards.
4. As you define your search filters, CA DataMinder generates a SQL search expression. If you have the 'Events: Allow unrestricted SQL searches' administrative privilege, you can click the SQL tab to edit this expression directly.

   Note: If you write your own search expression, refer to the SQL requirements (see page 51). Also, the handling for wildcards and other special characters, plus the requirements when specifying user or group names, are the same as for event searches.

5. Save the search definition.

   Saved searches are listed under the Custom Searches folder in the Administration console.

6. Click Search Now to run the search. Or choose Search > Search Now.

   Items matching the search criteria are shown in the Search tab.

More information:

Wildcards (see page 48)
Backslashes (see page 49)
Searching by User Name (see page 50)
Searching by User Group (see page 50)
SQL Search Expressions (see page 51)

Wildcards

Note: All search fields that require text input support ? and * wildcards.

Supported wildcards

CA DataMinder supports the familiar ***** and **?** wildcards. It also supports **%** and **_** (underscore) wildcards, as used in SQL database queries.

When defining a search, you can use these wildcards in any field that requires text input. In these fields, you can substitute % or * for zero or more characters; you can substitute _ or ? for a single character.

Automatic wildcards

When you enter any text in a search filter, CA DataMinder adds leading and trailing % wildcards automatically when you enter a text value. For example, CA DataMinder interprets:

- **rimm** as equivalent to **%rimm%**.

  This example filters the search to only include users such as spencerrimmel.

- **ma** as equivalent to **%ma%**.

  This example filters the search to only include user groups such as 'Management' or 'Direct Marketing'.

Manual wildcards

You can manually enter % or * and _ or ? as internal wildcards within any text string in any search filter. For example:

- **spen%rim** or **spen*rim** returns a range of matching names, such as spencerrimmel or spenserrimel.
- **spen_errimmel** or **spen?errimmel** limits the possible matches to a more narrow range of names such as spencerrimmel or spenserrimmel. It does not return names such as spenserrimel.

Literal wildcards

To search for literal % or * and _ or ? wildcard characters, prefix them with a backslash. For example:

- **25\%** detects "25%"
- **24*7** detects "24*7"
- **my_file.xls** detects "my_file.xls"
- **What next\?** detects "What next?"

Backslashes

The \ backslash character has a special meaning in CA DataMinder search fields (it is used when searching for literal wildcard characters). To search for literal backslashes, you can normally enter these as ordinary characters but in some situations they require special handling.

If your search text includes a backslash (for example in a user name such as unipraxis\lsteel or a path such as \Sales\2003Q1.xls) CA DataMinder detects that the backslash is an ordinary character and no further action is necessary.

But if you want to detect a literal backslash that is followed by a wildcard character (% * _ ?), you prefix the backslash with another backslash. For example, to search for this captured text:

```
'C:\*\Q1_sales.xls'
```

You must enter this search text:

```
C:\\*\Q1_sales.xls
```

Where \\ detects the first literal backslash; because the second literal backslash is followed by a standard character ('Q'), it does not need a backslash prefix.

Searching by User Name

When searching for data, if you filter your search by user name, be aware of the following:

Domain Prefixes

By default, CA DataMinder uses Windows authentication to create user accounts. This means you must prefix user names with the domain when searching for user-specific items. For example, to refer to SpencerRimmel in the Unipraxis domain, the syntax is:

```
WHERE WgnUser.NativeUser='Unipraxis\SpencerRimmel'
```

Note: You do not need to supply a domain prefix if the user account was created manually by an administrator.

Oracle Requirements

When searching for data, user names are not usually case-sensitive. But if your CMS uses an Oracle database engine and you enter a custom search expression in the SQL tab, user names are case-sensitive.

For example, user SpencerRimmel can log on to the Administration Console by typing spencerrimmel or SPENCERRIMMEL. But if you want to search for this user, you must type SpencerRimmel in the SQL tab of the Administration Search dialog.

Note: This applies only to the SQL tab. On other search tabs, the User Name field is not case-sensitive.

Searching by User Group

Important! If you specify a group, the search retrieves events associated only with users in the specified group. It does not retrieve events associated with users in subgroups of the specified group.

For example, if you are searching for e-mail events and you select a specific group as a search filter, CA DataMinder does not retrieve e-mails associated with users belonging to subgroups of the specified group.

SQL Search Expressions

Search for Data - SQL Requirements

CA DataMinder is optimized to allow fast, safe and flexible database searching. But if you want to edit the SQL search expression that CA DataMinder generates automatically, or if you want to write your own customized SQL search expressions, be aware of the following issues:

Note: You can only edit the SQL search expression if you have the Events: Allow unrestricted SQL searches privilege.

SELECT keyword

CA DataMinder will only recognize search expressions that begin with SELECT. To maintain database integrity, it will not allow other keywords such as DROP, INSERT, UPDATE or DELETE.

Result sets

CA DataMinder will only return objects from the first database table specified after the FROM operator. That is, the result set of a search must comprise a single table of a supported type.

Furthermore, CA DataMinder supports 'entire row select' on those supported tables. So for example, within a single search expression, you cannot search for all machines and all users.

In effect, this means that all search expressions must comply with the following syntax examples:

```
SELECT * FROM WgnMachine
```

```
SELECT i.* FROM WgnUser i
```

Arithmetic operators

CA DataMinder supports the following arithmetic operators, > < <= >= and <>. You can use these operators in conjunction with the Event Size and Date filters, and also when limiting result sets chronologically.

Dates

The search filter tabs let you quickly define date ranges, without needing to edit the SQL search expression directly. But if you want to run repeat searches using different date ranges, you may find it faster to edit the appropriate SQL lines directly before running each search. Detail:

1. Use the search filter tabs to find all e-mail events captured between two specific dates.
2. Now go to the SQL tab and click Edit to customize the automatically-generated SQL search expression.
3. Find the lines similar to these:

   AND e.EventTimestamp>={d '2002-08-01'} This defines the start date.

AND e.EventTimestamp<{d '2002-08-02'} This defines the end date.

4. Edit the dates directly and click Search Now.

Limiting result sets chronologically

CA DataMinder supports search expressions that limit the size of a result set. When used in combination with chronological result sorting, this enables you to retrieve, for example, the 25 most recent Web page warnings.

SQL Server and Jet

Use a SELECT TOP expression. The syntax must comply with the following example:

```
SELECT TOP 25 * FROM WgnEvent
  ORDER BY EventTimeStamp desc;
```

Oracle8i

Because SELECT TOP expressions are not supported, the syntax must take this format:

```
SELECT * FROM
  (SELECT * FROM WgnEvent
  ORDER BY EventTimeStamp desc)
  WHERE rownum <=25;
```

More information:

Supported Table Types - Administration Data Searches (see page 52)

Supported Table Types - Administration Data Searches

When writing your own SQL search expression to search for administration data, the following tables are supported tables:

- Wgn3User
- WgnGroup
- WgnMachine

Note: You can only edit the SQL search expression if you have the Events: Allow unrestricted SQL searches administrative privilege.

More information:

Search for Data - SQL Requirements (see page 51)

Saved Searches - Administration Data

You can save searches for users, groups or machines. This allows you to run repeat searches and share search expressions with your colleagues.

To save a custom search

1. Define a search (see page 45) as normal in the Administration Search dialog.
2. Choose Search, Save Search.

   The search file is saved on the computer hosting the Administration console and is only available in the Administration console on that computer.

To open a saved search

1. Log on to the Administration console on the computer where your custom search is saved.
2. Expand the Searches, Custom Searches branch.
3. Right-click the search you want and click Edit.

Search Results: Available Actions

When viewing the results of an administration search, various actions are available:

Users

Right-click any user in the results pane and choose from the available actions:

Locate

Expands the User Administration branch and locates the user within the user hierarchy.

View Summary

Displays summary details about the user, including when the account was created, session details, and policy details. From the User Summary dialog, you can launch the Policy Editor to directly view or edit this user's policy.

Rename

Allows you to rename the user name (the name used by the user account, not the full name).

Move Item

Allows you to choose a new parent group for the current user. Moving users can affect their policy and may raise security issues.

Properties

Allows you to edit user names, roles, attributes and assign administrative privileges. You can also update the e-mail addresses associated with the current user.

Copy to Clipboard

Copies the selected results to the clipboard; from there, you can paste them into, for example, a spreadsheet or Microsoft Word document.

Note: To move or rename users, or to view or edit policies, your CA DataMinder user account needs appropriate administrative privileges.

Groups

Right-click any group in the results pane and choose from the available actions. These include:

Locate

Expands the User Administration branch and locates the group within the user hierarchy.

View Summary

Displays summary details about the group, including group members and policy details. From the Group Summary dialog, you can launch the Policy Editor to directly view or edit this group's policy.

New User

Opens the New User dialog to add a new user to the current group.

New Group

Opens the New Group dialog to add a child group to the current group.

Set As Default

Sets the current group as the default group. New users who create their own CA DataMinder accounts are added automatically to the default group. This is effectively a holding group until you can move new users into more appropriate groups.

Export Hierarchy to File

Exports the contents of the current group to a file compatible with Account Import or a spreadsheet, or to an XML file. You specify the export options in the resulting dialog.

Rename

Allows you to rename the group.

Move Item

Allows you to choose a new parent group for the current group. Note that moving groups can affect their policy and may raise security issues.

Copy to clipboard

Copies the selected results to the clipboard; from there, you can paste them into, for example, a spreadsheet or Microsoft Word document.

Note: To move or rename groups, or to view or edit policies, your CA DataMinder user account needs appropriate administrative privileges.

Machines

Right-click any group in the results pane and choose from the available actions. These include:

Locate

Expands the Machine Administration branch and locates the client machine or server within the machine hierarchy.

View Summary

Displays summary details about the machine, including when the account was created, session details, and policy details. From the Machine Summary dialog, you can launch the Policy Editor to directly view or edit this machine's policy.

Edit/View Policy

Launches the Policy Editor to directly view or edit this machine's policy.

Edit Common Client Policy

For client machines only. Launches the Policy Editor to edit the Common Client Policy. By default, new client machines inherit this policy.

Edit Common Gateway Policy

For gateways. Launches the Policy Editor to edit the Common Gateway Policy. By default, new gateways inherit this policy.

View Logfiles

Displays the Logfile View dialog, showing available logfiles for the current machine.

Machine State

Displays the Machine State dialog. From here, you can suspend machines or resume suspended machines.

Delete

Deletes the current machine account. Note that deleted accounts are retained in the database for auditing purposes.

Move Item

Allows you to choose a new parent server for the current machine.

Suspend

Suspends the current machine. Certain CA DataMinder operations continue or remain available on a suspended machine.

Resume

Resumes the current machine (if suspended).

Copy to clipboard

Copies the selected results to the clipboard; from there, you can paste them into, for example, a spreadsheet or Microsoft Word document.

Note: To move or rename machines, or to view or edit policies, your CA DataMinder user account needs appropriate administrative privileges.

More information:

Move Users Between Groups (see page 202)
Default Group (see page 200)
What Operations are Still Available on Suspended Machines? (see page 141)
User Properties (see page 204)

Chapter 4: CMS Administration

This section contains the following topics:

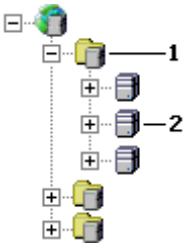
Multiple CMSs (see page 57)
CMS Groups (see page 58)
Connect to a CMS (see page 58)
Enable Single Sign-on (see page 60)
Security Models (see page 60)
Suspend or Resume a Machine (see page 64)
Backing Up and Restoring the CMS (see page 65)
Manage System Files (see page 69)

Multiple CMSs

If you deploy multiple CMSs, each serving a separate cluster of CA DataMinder machines, you can connect to each CMS from a single Administration console. For example, you can administer users, browse captured data or edit user policies on any CMS listed in the Administration console.

To connect to a different CMS

Expand the CMS group (**1**) select the CMS you want (**2**).



More information:

CMS Groups (see page 58)
Connect to a CMS (see page 58)

CMS Groups

To simplify your administration routine, you can organize CMSs into hierarchical groups. You can create as many groups as you need. For example, you can create separate CMS groups for different geographical regions.

To add a new CMS group

You can organize CMS's into groups to simplify your administration routine. Choose File, Add CMS Group or click in the toolbar.

To add a CMS

Before you can administer an existing CMS, you first need to add it to your Administration Console.

1. Choose File, Add CMS or click in the toolbar.
2. In the resulting dialog, browse to the server you want.

To reorganize CMSs and CMS groups

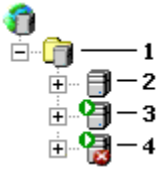
You can move a CMS from one parent group to another using drag-and-drop. You can also drag-and-drop an entire group from one parent to another.

More information:

Multiple CMSs (see page 57)

Connect to a CMS

Icons in the CMS tree indicate the status of each CMS:



1 My Servers icon. **2** Disconnected CMS. **3** Connected CMS. **4** Suspended CMS

To connect to a CMS

1. In the CMS tree, select a disconnected CMS .
2. Right-click the CMS and choose Connect.
3. Supply your logon user name and password.

To disconnect from a CMS

You may want to disconnect from a CMS in order to log on to the CMS as a different user, or simply to free up resources on the local server.

1. In the CMS tree, select a connected CMS .
2. Right-click the CMS and choose Disconnect.

To connect to a CMS as a different user

If necessary, you can disconnect from and reconnect to a CMS in one easy step. You may want to log on as a different user for reasons of security.

1. In the CMS tree, select the CMS you want to connect to.
2. Right-click the CMS and choose Connect As.
3. Supply the logon user name and password you want to use.

More information:

Multiple CMSs (see page 57)
Suspend or Resume a Machine (see page 64)

Enable Single Sign-on

If required, you can configure CA DataMinder so that users skip the logon dialog when they start up a CA DataMinder console.

Instead of the user supplying credentials to access the console, CA DataMinder relies on the fact that the user has successfully logged into Windows as sufficient authorization to allow them to log on to the CA DataMinder account of the same name. In all other respects, the authentication process is identical to using a logon dialog.

To configure CA DataMinder to use single sign-on

1. Edit the CMS machine policy.
2. In the Central Management Server policy folder, set Allow Single Sign-on? to True.

   Note: Be aware of the following:

   - The administrative privilege 'Admin: Use single sign-on' allows a user to log on with single sign-on, even if single sign-on is disabled on the CMS.
   - This functionality requires that users wanting to run consoles have CA DataMinder account names prefixed with their domain, for example, UNIPRAXIS\lyndasteel.

Security Models

Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database.

You can choose which security models are available on your CMS. You can also have multiple security models active at the same time, though each reviewer is linked to a single model.

For example, some reviewers may only be permitted to see events linked to users in their own management group. Other reviewers may only be permitted to see specific types or categories of events.

CA DataMinder supports the following security models:

Management Group (Standard)

This is the default model, optimized to allow fast searching. It is based on the CA DataMinder user hierarchy.

It uses e-mail addresses (including synthesized addresses for participants in Web and Application Monitor events) to map participants to CA DataMinder users. Under this model, reviewers can only view events where at least one participant was in their management group when the event was captured.

Management Group (Standard, Self-Exclude)

This model prevents reviewers from seeing their own events. As above, reviewers can only view events where at least one participant was in their management group. However, under this model the search results also exclude any events in which the 'logged-on user' (that is, the reviewer) was a participant.

Management Group (Sender)

Under this model, when a reviewer runs an e-mail search, they can only view events where the e-mail sender was in their management group when the event was captured.

Important! This sender-centric security model is only appropriate for e-mail searches. Searches for other event types will return zero results.

Management Group (Sender, Self-Exclude)

This model prevents reviewers from seeing their own e-mails (or any other events) when they run a search.

As above, reviewers can only view events where the e-mail sender was in their management group. However, under this model the search results also exclude any events in which the 'logged-on user' (that is, the reviewer) was a participant.

Policy (Standard)

This model ensures that reviewers can only see specific types of event. For example, this model can be used to ensure that HR reviewers only see events that relate to HR issues such as employee behavior, while Legal reviewers only see events that relate to legal issues such as litigation threats or a breach of attorney client privilege.

The model is based on *policy classes*. For categorization purposes, you can associate individual triggers with a *policy class*, such as 'Employee Behavior' or 'Legal'. When a trigger fires, the policy class is stored with the associated event.

Likewise, each reviewer has a policy role. A *policy role* links a user to a collection of policy classes. In effect, the policy role determines which policy classes a user is permitted to see. When the user runs a search, the results only include events associated with these policy classes.

Policy (Standard, Self-Exclude)

This variant of the Policy model prevents reviewers from seeing their own events. As above, reviewers can see only specific types of event. However, the search results also exclude any events in which the reviewer was a participant

Hybrid Model: Management Group and Policy

If required, you can add a hybrid model on your CMS. This combines the Management Group and Policy models. Its effect is to restrict reviewers so they can only see specific types of event associated with users in their management group. For example, under this model a reviewer in the Legal team can only review legal events associated with members of their management group.

Unrestricted

This model is not subject to row level security (RLS). It permits reviewers to see any events when they run a search or report. Search results or reports are not restricted by policy class or the reviewer's management group.

This model is primarily required by CA DataMinder user accounts set up explicitly for use by external reporting tools when searching the Data Warehouse for events.

Note: You can only assign the Unrestricted security model to a CA DataMinder user if you have the 'Admin: Disable security model filtering' administrative privilege.

Important! Certain reports and the Review Queue are not designed for use with Policy security models. See the reference below for details.

More information:

Manage Security Models (see page 62)
Policy Security Models Not Compatible With Some Reports or Review Queue (see page 64)

Manage Security Models

Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database for events.

CA DataMinder supports multiple security models, including models based on management groups, variants of this original model (for example, to prevent reviewers reviewing their own e-mails), and policy-based models. You can choose which models are active on your CMS and multiple models can be active at the same time. However, each reviewer can only be linked to a single model. For example, some reviewers may only be permitted to see events linked to users in their own management group. Other reviewers may only be to see specific types or categories of events.

When you first install CA DataMinder, only one security model is active. This is the default security model, Management Group (Standard). You must enable other security models before you can assign them to reviewers.

You can manage security models in the Administration console.

To enable a security model on the CMS

1. Choose Tools, Manage Security Models.
2. In the Manage Security Models dialog, click Add.

3. In the Create Security Model dialog, you can configure the model you want. You need to:

   - Set the database user name. You must provide the name and password for a secure database account.

     CA DataMinder consoles use these credentials to connect to the CMS database when searching for events under the new security model.

     Important! Each security model must use its own database account. Security models cannot share the same database account.

   - Set the model type. You must choose from the available types, such Management Group (Sender).

     If required, you can add a hybrid security model. This combines two security models to filter the results when a reviewer searches for events.

To modify a security model

1. Choose Tools, Manage Security Models.
2. Select model you want and click Modify.

   You can now change the database user name or model type.

To remove a security model

1. Choose Tools, Manage Security Models.
2. Select model you want and click Remove.

   Any reviewers still assigned to this model will revert to the default security model. (Typically, this is the Management Group (Standard) model, although you can change the default model type.)

More information:

Security Models (see page 60)

Policy Security Models Not Compatible With Some Reports or Review Queue

Certain reports, particularly the compliance reports such the Repeat Offender report and Compliance Audit Report, are not designed for use with Policy security models. This is also true for the Review Queue feature and the associated Reviewer search.

These reports and the Review Queue are explicitly designed to be run in conjunction with the Management Group security models. That is, they return data about users in specific user groups.

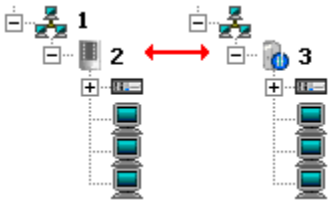
Important! We recommend that any users who need to run these reports or the Reviewer search are assigned to a Management Group security model, not to a Policy security model.

Suspend or Resume a Machine

You must have the 'Edit Machine Hierarchy' administrative privilege to be able to suspend or resume CA DataMinder machines,

To suspend or resume a CMS

1. Expand the Machine Administration branch (**1**) and select the CMS.
2. Do one of the following:
   - Right-click an active CMS (**2**) and choose Suspend.
   - Right-click a suspended CMS (**3**) and choose Resume.



To suspend or resume a gateway or client machine

1. Expand the Machine Administration branch and select the gateway or client you want.
2. Right-click the machine and choose Machine State.
3. In the resulting dialog, click Suspend or Resume.

More information:

Overview (see page 140)

Backing Up and Restoring the CMS

More information:

Overview (see page 65)
General Backup Tasks (see page 66)
Backup Tasks for SQL Server (see page 66)
Backup Tasks for Oracle (see page 67)
Restoring the CMS (see page 68)

Overview

How to back up a CMS

We recommend that you make a full backup of your CA DataMinder database on the CMS at least once per week, and incremental backups on a daily basis.

1. Back up essential registry keys on your CMS.
2. For SQL Server databases, set up maintenance plans for your system databases and your CA DataMinder database.

   For Oracle databases, set up a backup schedule.
3. Add the CA DataMinder data folder into your existing backup regime.

How to restore a CMS

1. Stop the CA DataMinder infrastructure.
2. Re-import the master encryption registry key that is used by the original installation.
3. Restore the CA DataMinder data folder.
4. Restore the CMS database.
5. Reinstall CA DataMinder on the CMS server.

More information:

General Backup Tasks (see page 66)
Restoring the CMS (see page 68)

General Backup Tasks

When you back up the CMS, you must perform these backup tasks irrespective of the type of database engine used on the CMS.

Backing up the CA DataMinder data folder

The CA DataMinder data folder holds all the configuration data and captured data used by your CA DataMinder installation. You need to incorporate this folder into your existing backup regime. We recommend you back up this folder every week. By default, when you install CA DataMinder this folder is added as a \Data subfolder in the installation folder, but you can rename it and locate it anywhere suitable on your network.

Backing up the master encryption registry key

The CMS uses a protected registry key to provide highly secure data management. If you need to restore the CMS, you will need to restore this registry key. To do this, CA DataMinder provides the data management utility wgnmgmt.exe for exporting and re-importing this key. Find this utility in the \Support folder on your CA DataMinder distribution media.

After installing your CMS, you must run wgnmgmt.exe on the CMS machine to export a password-protected file containing the necessary registry details. The command line syntax:

```
wgnmgmt e <filename> <password>
```

Where <filename> is the name of the target file, for example, master_encryption.dat. And <password> is the password you use to re-import the registry key. The password must be at least five characters long.

Important! Keep this file in a secure location, for example, on a floppy disk in a fire-proof safe.

Backup Tasks for SQL Server

Note: Backup and recovery procedures have been tested using Microsoft SQL Server 2000. These procedures may work

If your CMS uses a SQL Server database:

1. Back up the master encryption registry key.
2. Back up your SQL Server database.

   Please refer to your SQL Server documentation for details.
3. Back up your CA DataMinder data folder.

More information:

General Backup Tasks (see page 66)

Backup Tasks for Oracle

If your CMS uses an Oracle database:

1. Back up the master encryption registry key.
2. Back up your Oracle database.

   Please refer to your Oracle documentation for details. For example, you can find backup and recovery procedures in the *Oracle® Database 2 Day DBA* book and the *Oracle Database Backup and Recovery User's Guide*.
3. Back up your CA DataMinder data folder.

More information:

General Backup Tasks (see page 66)

Restoring the CMS

These instructions describe how to restore the CMS to a point-in-time. You may need to do this if your CMS suffers a hardware failure, for example.

How to restore the CMS

1. **Stop the CA DataMinder infrastructure.** Use the Computer Management utility in Windows. Expand the Services group and stop the service 'CA DataMinder Infrastructure'.

   Or you can stop the infrastructure service from a command line:
   `net stop wgninfra`

2. **Re-import the master encryption registry key**. This is the registry key used by the original installation. Run wgnmgmt.exe on the CMS server. The command line syntax is:

   `wgnmgmt i <filename> <password>`

   Where <filename> and <password> are the backup file and password you specified during the General backup tasks.

3. **Restore the CA DataMinder data folder**. Use your normal data-recovery procedures to restore the CA DataMinder data folder to your CMS. You can restore it to any suitable location on your network, and give it any name. You specify the name and location when you reinstall CA DataMinder (step 5).

4. **Restore the CMS database**. The procedure depends on your database engine:

   - For Oracle databases, create a recovery job for your CA DataMinder database using the Recovery wizard. See your Oracle documentation for details.
   - For SQL Server databases, restore your CA DataMinder database using the SQL Server Database Restore feature. See your SQL Server documentation for details.

   Note: If you are restoring after a complete system failure, you must recreate a login for CA DataMinder to use. For details, see the SQL Server guidelines in the *Database Guide*.

5. **Reinstall CA DataMinder on the CMS server**. Use the CA DataMinder installation wizard.

   - In the Database Accounts screen, enter the name and password for the login that CA DataMinder will use to manage the CMS database.
   - In the Data Folder screen, specify the name and location of the data folder that you previously recovered in Step 3.

More information:

General Backup Tasks (see page 66)

Manage System Files

If a problem occurs with your CA DataMinder installation, you may be instructed to examine system files stored in the CMS database. Analysis of the system files can often help CA technical staff diagnose the problem.

CA DataMinder system files include such items as iConsole search definitions, content registration agents, definition files for social security numbers, dynamic address lists and audit mail templates. CA DataMinder stores these system files in the CMS database. Each system file has two parts: the file metadata and the actual file content. The metadata includes such details as the file name and creation date. The file content itself comprises XML or binary data.

The Administration console includes the System File Explorer for managing system files. The System File Explorer is very similar to Windows Explorer and displays the internal file system within the CMS database. It lets you browse the internal file system to view, edit, and replace system files.

More information:

View System Files (see page 69)
Edit System Files (see page 70)
Replace System Files (see page 71)

View System Files

The Administration console lets you view system files in read only mode. Viewing these files in read only mode prevents you from accidentally deleting or modifying crucial data.

Note: You must have the 'Admin: Manage System Files' administrative privilege in order to view system files.

To view system files

1. Click a CMS in the Administration console.
2. Click Tools, View System Files.

   The System File Explorer appears.
3. Browse the system folders to find the file you want to view.
4. Right-click the file and do one of the following:
   - Click Open or Open With to view the file contents in Read Only mode.
   - Click Properties to view the file metadata and other details.

Edit System Files

You cannot edit system files directly in the CMS database. Instead, the Edit System Files feature in the Administration console lets you edit a *copy* of the system file. You can then import the edited copy onto the CMS, replacing the original system file.

Note: You must have the 'Admin: Manage System Files' administrative privilege to edit copies of system files.

To edit system files

1. Click a CMS in the Administration console.
2. Click Tools, Edit System Files.

   The System File Explorer appears.
3. Browse the system folders to find the file you want to view.
4. Right-click the file and click Open or Open With.

   A copy of the file opens in your preferred editor.
5. Amend the file and save the changes.

   The copy of the system file is saved to the folder you specify on the local server or a remote server. If necessary, you can now import this copy onto the CMS to replace the original system file.

Replace System Files

If you want to replace a system file with a different version, you must import a new version of the file. When you import a system file, the content of the original system file is replaced by the content of imported new file. However, the metadata of the original system file is retained.

For backup purposes, we recommend that you first export the original file to a folder on the local server or a remote server.

To export system files

1. Click a CMS in the Administration console.
2. Click Tools.
3. Click View System Files or Edit System Files.

   The System File Explorer appears.
4. Browse the system folders to find the file you want to export.
5. Right-click the file and click Export to copy the file from the CMS database to a folder on the local server or a remote server.

To import a system file

1. Click a CMS in the Administration console.
2. Click Tools.
3. Click View System Files or Edit System Files.

   The System File Explorer appears.
4. Browse the system folders to find the file you want to *replace*.
5. Right-click the file and click Import.

   The Import File dialog appears.
6. Browse to the file whose content you want to *import* and click Open

   The file content is imported, replacing the content of the original system file. The metadata of the original system file is *not* replaced.

Chapter 5: Content Registration

This section contains the following topics:

About Content Registration (Fingerprinting) (see page 73)
Fingerprinting Components (see page 74)
Content Agent Types (see page 75)
Using Content Agents to Detect Printed Files (see page 77)
Using Content Agents to Detect Spreadsheets (see page 78)
How to Set Up Content Agents (see page 79)

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 (see page 78) or printed files (see page 77).

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.

Content Agent Types

When you create a new content agent, you must choose its type. CA DataMinder supports the following types of content agent:

File Detection

These content agents can detect protected files in their entirety.

For example, if a user attaches a protected file, wholly unchanged, to an email or copies it to a USB drive, the content agent detects it.

Text Detection

These content agents can detect emails or files containing text copied from, or based on, a protected document. There are two aspects to these agents.

First, you must specify the agent accuracy. This depends on how much detail is stored in each document fingerprint, which in turn affects the size of the content index associated with the agent.

Second, you must specify how sensitive the agent is when checking suspected emails or documents for protected content.

Accuracy

You can choose how accurately your content agent can identify text extracted from a fingerprinted document.

The available settings (sentence, paragraph, page and so on) determine the level of detail stored in the fingerprint of a protected document. Specifically, these settings determine the size of each analyzable section in a protected document. The agent then generates a fingerprint for that document based on the most significant phrases in each section.

Agent Sensitivity

You can specify how sensitive the agent is to the loss, or potential loss, of protected files and documents. There are two methods for specifying the agent's sensitivity.

- Detect documents or their derivatives

  The agent can check for variants of protected documents, such as an early draft of a sensitive report.

  The agent can also detect documents that closely resemble a protected document. These include documents that have been deliberately modified (for example, by changing key phrases or re-ordering sections) in an attempt to circumvent CA DataMinder policy triggers.

- Detect extracts of documents

  Alternatively, the agent can check for extracts copied word-for- word from a protected document. You must specify the minimum size of these extracts.

At one extreme, you can set up an agent to detect any sentence, or any significant phrase, copied from a protected document and pasted into an email or another file.

At the other extreme, you can set up an agent to only detect emails or files that contain significant, extended passages copied from a protected document, equivalent to a several paragraphs or a full page of text.

Plain Text Embedded File Agents Are Superseded

Note: CA DataMinder 12.5 originally included support for Plain Text Embedded File content agents. These agents have since been superseded by Text Detection content agents.

Plain Text Embedded File content agents could detect the complete body text of a registered plain-text document. For example, the agents could detect a document with sensitive plain-text content (such as source code) if a user embedded the document in another document or in the body of an email.

However, CA DataMinder no longer allows you to create new Plain Text Embedded File agents, although existing agents will continue to work. Instead, we recommend that you replace your Plain Text Embedded File agents with the new Text Detection agents.

Text Detection agents represent a significant improvement over the old Plain Text Embedded File content agents. Previously, users could easily circumvent Plain Text Embedded File content agents by adding a minor text change to a protected document. Now you can set up Text Detection agents to detect, for example, variants of a protected document or attempts by a user to copy an extract from a protected document into an email or an attachment.

Using Content Agents to Detect Printed Files

CA DataMinder content agents can usually detect when a user tries to print a protected file. When this happens, the content agent invokes a Data In Motion trigger to, for example, block the print job. However, there are some limitations depending on the file type:

Text files

These include Microsoft Word and PDF documents.

Content agents **can** detect when a user tries to print extracts from a protected text file. However, an agent can only do this if it is configured to detect emails or files containing at least two-thirds of the text content from a protected document.

In practical terms, this means that the agent's Evaluation properties must use the 'Detect documents or their derivatives' method with the percentage similarity set to 70% or **lower**.

Note: If you choose a percentage similarity higher than 70%, the agent will be unable to match a print job to a protected document because of the presence of extra data such as print headers.

Spreadsheets and tables

These include Microsoft Excel files and information stored in tables in Microsoft Word documents.

Content agents **cannot** detect when a user tries to print a protected spreadsheet. Likewise, they cannot detect when a user tries to print a table copied from a protected file.

Images

These include Microsoft Visio drawings and all other image files, including PNGs, GIFs, and JPEGs.

Content agents **cannot** detect when a user tries to print protected Visio drawings or other images.

Presentations

These include Microsoft PowerPoint files.

Content agents **can** detect when a user tries to print slides from a protected presentation. However, if the slides have a decorative background, such as an image, this can sometimes interfere with the agent's ability to detect the text content. In turn, this may mean that policy triggers do not fire.

Using Content Agents to Detect Spreadsheets

CA DataMinder content agents can usually detect when a user tries to copy or send a protected spreadsheet. For example, you can use content agents to block emails where the sender has attached a protected spreadsheet.

File Detection and Text Detection content agents can both detect protected spreadsheet files if they are unchanged. For example, they can detect when a user attaches the spreadsheet to an email.

Text Detection agents can also detect protected spreadsheets with minor edits (for example, a spreadsheet that contains some cells with updated values). In addition, they can detect when a user copies multiple rows from a protected spreadsheet into a new spreadsheet.

However, Text Detect agents cannot reliably detect when a user copies cell ranges from a protected spreadsheet into a different document format. For example, they may fail to detect when a user copies a range of cells into an email. This is particularly likely if the copied cells include hidden rows or columns because the pasted cell range omits the hidden cells and so no longer matches the spreadsheet fingerprint.

How to Set Up Content Agents

A registered content agent can quickly detect when a user tries to send or copy a protected file. To do this, it compares the file's digital fingerprint with the fingerprints of files that it is protecting.

To roll out content agents across your CA DataMinder enterprise

1. Create your content agents. Do this in the Administration console.
2. For each agent, you must specify which files it protects and its index type.

   For Text Detection agents, specify the agent accuracy and detection thresholds.

   Note: If you later change or extend the files protected by a specific content agent, you must rebuild the index and republish the content agent.
3. Build an index for each content agent.

   The index contains fingerprints of the files you want the agent to protect.
4. Publish the content agent.

   This process pushes the content index file onto the CMS and makes a fully functioning content agent available to your policy engines and endpoint agents.

   Note: Until an index has been built and the content agent has been published, you cannot use the agent in user policy. Any trigger that uses an unpublished content agent will be unable to detect fingerprinted files.
5. Assign content agents to triggers in your user policies.

More information:

To create a content agent (see page 79)
To add files that you want to protect (see page 82)
Build a Content Index (see page 82)
To publish a content index (see page 83)
Set up Content Agent Triggers (see page 84)

To create a content agent

Follow these steps:

1. In the Administration console, expand the Content Registration branch.
2. Right-click the Agents folder and choose Create Content Agent.

3. In the Select Agent Index Type dialog, choose the agent type:

   Exact File Detection

   These content agents can detect protected files in their entirety. For example, if a user attaches a protected file, wholly unchanged, to an email or copies it to a USB drive, the content agent detects it.

   Text Detection

   These content agents can detect emails or files containing text copied from, or based on, a protected document.

   There are two aspects to these agents. First, you can specify how much detail is stored in each document fingerprint. This affects the size of the content index associated with the agent. Second, you can specify how sensitive the agent is when checking suspected emails or documents for protected content.

4. In the Agent Properties dialog, supply the following details:

   General tab

   Specify the agent name and description and the Index Builder Machine. This can be any server on your network hosting the CA DataMinder File Scanning Agent.

   (Optional. Text Detection agents only) Specify subsidiary agents to reduce the number of false positives. These agents identify and exclude from processing text extracts that are deemed benign or acceptable, such as corporate disclaimers.

   Filter tab

   (Optional) Specify the folder and file options, such as whether to fingerprint hidden files or files in subfolders.

   Build tab

   (Text Detection agents only) Specify how much detail is stored in the fingerprint of a protected document. The more detailed the fingerprint, the more reliably an agent can recognize content originating from that document. However, a content index containing highly detailed fingerprints can be very large indeed.

   For details, see What Level of Accuracy Do I Need? (see page 81)

   Evaluation tab

   (Text Detection agents only) Specify how sensitive the agent is to the loss, or potential loss, of protected files and documents. There are two methods for specifying the agent's sensitivity:

   - The agent can check for variants of protected documents or documents that closely resemble a protected document.
   - Alternatively, the agent can check for extracts copied word for word from a protected document. You can specify the minimum size of these extracts.

What Level of Accuracy Do I Need?

(Applies to Text Detection content agents only)

The accuracy of an agent depends on the level of detail in the document fingerpints. If you include more detail in a document's fingerprint, the agent is more accurate. That is, the agent can recognize content originating from that document more reliably.

At one extreme, you can generate a fingerprint that covers every **sentence** in a protected document. Agents based on highly detailed document fingerprints like these are the most accurate.

At the other extreme, you can generate a fingerprint that slices the document into sections analgous to a **page**. This fingerprint only covers the most significant phrases within each page-sized section. Agents based on these fingerprints are less accurate, but have far smaller indexes.

Note: A content index containing highly detailed (sentence-level) fingerprints can be very large indeed. In fact, these indexes can be *eight* times larger than comparable indexes containing the least detailed (page-level) fingerprints. Such large indexes can be a particular problem if you enable content agent triggers on your CA DataMinder endpoint machines, because each endpoint machine maintains a copy of each agent's content index.

Supplementary Agents to Reduce False Positives

(Applies to Text Detection content agents only)

A subsidiary content agent operates in conjunction with a parent agent to reduce the number of false positives detected by the parent content agent. The subsidiary agent identifies and excludes from processing any text that is deemed benign or acceptable, such as corporate disclaimers.

For example, if you have fingerprinted a series of confidential reports, each of which includes a corporate disclaimer, you do not want your content agent to positively flag every email or file containing this disclaimer. You can prevent this happening by specifying a subsidiary agent that has been configured to detect these disclaimers. When the subsidiary agent detects a disclaimer, the associated text is excluded from normal processing by the parent content agent.

You can designate one or more supplementary content agents when you create a Text Detection content agent. You can then create an index of digital fingerprints for each supplementary agent in the normal way. For example, you may want to create a text document containing your corporate disclaimer and generate a fingerprint of this document.

To add files that you want to protect

After creating a content agent, you must specify which folders and files it will protect.

Note: If you later change or extend the files protected by a specific content agent, you must rebuild the index and republish the content agent.

Follow these steps:

1. In the Administration console, expand the Content Registration branch.
2. Right-click the agent and choose Add Location.
3. In the Add Location dialog, browse to the folders and files you want to protect.

   Note: CA DataMinder can fingerprint files contained within zipped files.

Build a Content Index

Before you can use a content agent, you must create an index of digital fingerprints for all files protected by the agent. Until an index has been built and the content agent has been published, the agent cannot be used in user policy. That is, any content agent trigger that uses an unpublished agent will be unable to detect fingerprinted files.

After adding the files that you want a content agent to protect, you must build an index of these files.

Follow these steps:

1. Select the agent in the Content Registration screen.
2. Click the ▶ Start Build button.

   This launches a scanning job. If you need to cancel the job, click the ■ Stop Build button.

   When the build process is complete, you must publish the associated content agent.

Rebuild a Content Index

If you change or extend the files protected by a specific content agent, you must rebuild the index and republish the agent.

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.

The rebuild procedure is the same as when you build an index for the first time.

Follow these steps:

1. (Optional) Purge the content index.

   If you have made substantial changes to the files protected by a content agent, we recommend that you first purge the index to remove all digital fingerprints and then rebuild it.

2. Select the agent in the Content Registration screen.
3. Click the Start Build button.

   When the build process is complete, the index contains the original list of protected files plus any new or modified files.

4. Re-publish the updated content agent.

To purge a content index

If you have made substantial changes to the files protected by a content agent, we recommend that you purge the index to remove all digital fingerprints and then rebuild it.

Follow these steps:

1. Select the agent in the Content Registration screen.
2. Click the Purge button.

   You now need to rebuild the index.

To publish a content index

After building your content index, you must publish the content agent.

Follow these steps:

1. Select the agent in the Content Registration screen.
2. Click the Publish button.

Set up Content Agent Triggers

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.

   Reviewers will search for 'fingerprint events' using these trigger names and policy classes.

Chapter 6: Data At Rest Scans

This section contains the following topics:

Data At Rest Scans (see page 85)
Manage Scanning Jobs (see page 86)
Create a Scanning Job (see page 88)
Scheduled Scanning Jobs (see page 89)
Database Scanning Jobs (see page 90)
Command Line Scanning Jobs (see page 91)
Import Version 6.0 Scanning Jobs (see page 92)
Purge the Scan Database (see page 92)
Binary Data Handling (see page 93)
Specify FSA Server Properties (see page 96)
FSA User Accounts (see page 97)

Data At Rest Scans

Data At Rest scans use the File Scanning Agent (FSA) to scan and analyze data and apply Data At Rest policy triggers. Data At Rest scans can analyze the text content of:

- Files saved in local and remote file systems.
- Microsoft Exchange Public Folder data, such as, calendar events, tasks, or journal entries.
- Microsoft SharePoint items, such as tasks or discussion boards.
- Database records.

Note: For full details about deploying the FSA, see the *Stored Data Integration Guide*; search for 'FSA'.

Manage Scanning Jobs

In the Administration console, you can perform the following tasks.

Create a scanning job

Right-click a file scanning server and click Create New Job.

Run or restart a scanning job

Right-click a scanning job and click Run Job Now.

If you restart a stopped job, CA DataMinder ignores items that have already been scanned in the current job. To do this, CA DataMinder performs hash checks to identify those files that can be excluded from the scan when it restarts. However, these hash checks can take a long time for very large scanning jobs.

Note: For each scanned item, the scan database contains a hash to uniquely identify that versin of the file plus its 'last scanned' date.

Note: You can also run scanning jobs from a command line.

Stop a scanning job

Right-click a scanning job and click Stop Job.

Reschedule a scanning job

Right-click a scanning job and click Schedule.

The Schedule Job dialog appears.

Clone or copy a scanning job

The Clone and Copy tools let you quickly create multiple scanning jobs. Right-click a scanning job and click:

Clone

Creates a new scanning job on the current file scanning server.

The new job has identical settings to the existing job, but with a different name.

Copy To

Copies the current scanning job to a different file scanning server. The new job has the same name and identical settings to the existing job.

After both Copy and Clone operations, you can customize the settings in the new job. For example, you can specify different scan locations.

Import a scanning job

Click a file scanning server and click Import Job File. You can select the XML scanning job definition that you want to import.

You may need to import scanning jobs if you have upgraded from CA DataMinder 6.0.

View scan logs

CA DataMinder maintains scan logs for each scanning job, each file scanning server, and each FSA stub, wgnfstub.exe. (The FSA Remote Connector uses an FSA stub.) To view:

Job logs

Right-click a scanning job and click View File Scanning Logfiles.

Server logs

Right-click a file scanning server and click View File Scanning Logfiles.

FSA stub logs

You cannot view these logs from the Administration console. These logs are saved to a WgnFStb_<date>.log file on the machine hosting wgnfstub.exe. These logs are saved in CA's \data\log subfolder of the Windows All Users profile.

More information:

Database Scanning Jobs (see page 90)
Scheduled Scanning Jobs (see page 89)
Import Version 6.0 Scanning Jobs (see page 92)

Create a Scanning Job

To create a scanning job

1. On the Administration console host machine, log on to Windows as the FSA Job Setup User.
2. Click Data At Rest Scans or CCS Preclassification Scans.
3. Right-click a file scanning server and click Create New Job.

   This launches the Scanning Job Definition wizard. The wizard steps you through the job configuration.
4. Enter the job settings in the wizard screens.

   The number of screens depends on the type of scanning job.
5. Click Finish in the final wizard screen.

   The Schedule Job dialog appears.
6. Specify when and how often the scanning job runs.

More information:

Database Scanning Jobs (see page 90)
FSA User Accounts (see page 97)
Scheduled Scanning Jobs (see page 89)

Scheduled Scanning Jobs

You can schedule scanning jobs for the FSA and CFSA.

FSA scanning jobs

You define a job schedule when you create a scanning job. After you click Finish in the final wizard screen, the Schedule Job dialog appears.

To modify the schedule for an existing scanning job, right-click a scanning job and choose Schedule.

In both cases, you must specify the FSA Run As user.

Important! When a scheduled scanning job is running, it is essential that nobody logs onto the target machine using the same account as the FSA Run As user!

CFSA scanning jobs

The Client File System Agent (CFSA) can scan local files and folders. You define the CFSA scan schedule in the local machine policy.

In the Client File System Agent, Data At Rest Protection, File System Scan Configuration policy folder you can specify the start day, start time, and frequency.

More information:

FSA User Accounts (see page 97)
Client File System Agent Settings (see page 180)

Database Scanning Jobs

You can set up FSA jobs to scan databases. Specifically, the FSA can scan columns in database tables that contain text or binary data. Binary data refers to documents (such as MS Word files).

What are database events?

When the FSA scans a database table, the scanned data is written to XML blob files. The FSA then passes these blob files to policy engines for processing.

Policy engines then apply Data At Rest triggers to the scanned data. If a trigger fires, a database event is generated and stored on the CMS. You can view these events in the iConsole; they are indicated by icons in the Search Results screen.

How does the FSA create database events?

By default, all scanned data in the table (each column for every row) is written to a single XML blob file and stored as a single event. However, for very large database tables, this is clearly undesirable. Instead, you can configure the FSA to slice the scanned data into smaller, more easily manageable events.

For example, you can specify a maximum number of rows per event, or a maximum size (in KB) per event. You can also configure special handling for binary data; for example, if a database table contains MS Word documents, you can specify that these documents are stored as attachments to database events.

How does the FSA connect to a database?

When you create a scanning job, the FSA generates a database connection string, based on the detail that you supply in the Job Definition wizard.

Important: If scanning Oracle databases, be aware that Oracle user, schema and table names are case-sensitive when you specify the connection string!

What data is captured?

When setting up a database scanning job, you can specify how binary data is handled.

Similarly, when you set up user policies, the Capture File Details? setting in each Data At Rest capture action determines what data is captured and stored on the CMS.

More information:

Binary Data Handling (see page 93)

Command Line Scanning Jobs

You can run FSA scanning jobs from a command line. First, you create a job using the scanning job definition wizard. Then you reference this job in an FSA command.

In practice, you only run scanning jobs from a command line when scanning a database. This is for security reasons. The command line method allows you to avoid storing database logon credentials in the job definition.

Example command

The command syntax is shown below. This command runs a database scan and prompts you for the logon credentials that the FSA will use to access the target database objects:

```
wgnfstub /job:<job name> /user /password
```

Where:

<job name>

Is the name of an existing scanning job. You specify job names in step 1 of the job definition wizard.

/user and /password

(Optional) The purpose of these parameters is to avoid the security risk of storing database credentials in a scanning job definition.

If these parameters are used, the FSA prompts you for the logon credentials that it will use to access the target database objects.

More information:

Database Scanning Jobs (see page 90)

Import Version 6.0 Scanning Jobs

Importing version 6.0 scanning jobs

For CA DataMinder r12.0, the underlying XML schema for scanning job definition files has been amended. If you have scanning jobs defined using version 6.0 of the CA DataMinder product, you must first import these jobs onto the FSA before you can run them. When you import 6.0 scanning jobs, the FSA automatically updates them to use the new r12.0 job schema. You can then run these jobs as normal.

Importing 6.0 job files

To import a version 6.0 scanning job file

1. In the FSA screen of the Administration console, select an FSA server and choose Edit > Import Job File.
2. This launches the Import FSA Job Definitions dialog. Browse to the XML job file that you want to import.
3. Each individual job defined in the 6.0 job file is added to the FSA screen. Note that the FSA creates a separate new job file for each individual job extracted from the 6.0 job file.

More information:

Database Scanning Jobs (see page 90)

Purge the Scan Database

To purge the scan database completely

Right-click a file scanning server and click Purge Scan Database.

The FSA purges *all* records from the scan database on the specified server.

To purge a scnning job

Right-click a scanning job and choose Purge Scan Database.

The FSA only purges records for the selected scanning job.

More information:

Database Scanning Jobs (see page 90)
FSA User Accounts (see page 97)
Scanned File Database (see page 93)

Scanned File Database

The FSA uses a scanned file database (also known as the 'scan database') to track the status of each file in a scanning job. For each scanned file, the database contains a hash to uniquely identify that version of the file plus its 'last scanned' date.

For scheduled scanning jobs, the FSA checks the hashes in the scanned file database to determine whether a file has changed or moved since the last scan. This allows the FSA to skip files which have not changed.

Similarly, if a scanning job gets interrupted (that is, it cannot finish scanning all the required files because, for example, there is a network or system failure), when the job next runs the FSA checks the hashes in the database and skips any files which have not been modified since they were last scanned.

Binary Data Handling

When setting up a database scanning job, you can specify special handling for binary data. For example, if a database table contains MS Word documents, you can specify that any documents found are stored as attachments to the resulting database event.

Binary data options

The following binary data options affect the events created by the FSA:

- Store binary data as event attachments = True or False
- Only store database rows with columns containing binary data = True or False
- Store rows containing binary data as individual events = True or False

Example Database Table

In this example table, column C contains binary data (in this case, Microsoft Word documents of varying size):

	Col.A	Col.B	Col.C	Col.D
Row 1	data	data		data
Row 2	data	data		data
Row 3	data	data		data
Row 4	data	data	X	data
Row 5	data	data		data
Row 6	data	data	X	data

Store Binary Data as Event Attachments = True

If you store binary data on the CMS as event attachments, the binary data options affect the events created by the FSA in the example database table as follows:

Only store database rows with columns containing binary data = True

Only rows with binary data are stored.

Store rows containing binary data as individual events = True

Only rows with binary data are stored and they are stored as individual events. The FSA generates four events:
Event1 contains data for row 1; plus attachment
Event2 contains data for row 2; plus attachment
Event3 contains data for row 3; plus attachment
Event4 contains data for row 5; plus attachment

Store rows containing binary data as individual events = False

Only rows with binary data are stored, but they are not stored as individual events. The FSA generates one event:
Event1 contains data for rows 1, 2, 3, and 5; plus four attachments

Only store database rows with columns containing binary data = False

All rows are stored.

Store rows containing binary data as individual events = True

All rows are stored, but rows with binary data are stored as individual events. The FSA generates five events:
Event1 contains data for rows 4 and 6
Event2 contains data for row 1; plus attachment
Event3 contains data for row 2; plus attachment
Event4 contains data for row 3; plus attachment
Event5 contains data for row 5; plus attachment

Store rows containing binary data as individual events = False

All rows are stored, but rows containing binary data are not stored as individual events. The FSA generates one event:
Event1 contains data for rows 1 through 6; plus four attachments

Store Binary Data as Event Attachments = False

If you do not store binary data on the CMS as event attachments, the binary data options affect the events created by the FSA in the example database table as follows:

Only store database rows with columns containing binary data = True

Only rows with binary data are stored.

Store rows containing binary data as individual events = True

Only rows with binary data are stored and they are stored as individual events. The FSA generates four events:

Event1 contains data for row 1; no attachment

Event2 contains data for row 2; no attachment

Event3 contains data for row 3; no attachment

Event4 contains data for row 5; no attachment

Store rows containing binary data as individual events = False

Only rows with binary data are stored, but they are not stored as individual events. The FSA generates one event:

Event1 contains data for rows 1, 2, 3, and 5; no attachments

Only store database rows with columns containing binary data = False

All rows are stored.

Store rows containing binary data as individual events = True

All rows are stored, but rows containing binary data are stored as individual events. The FSA generates six events:

Event1 contains data for row 1; no attachment

Event2 contains data for row 2; no attachment

Event3 contains data for row 3; no attachment

Event4 contains data for row 4

Event5 contains data for row 5; no attachment

Event6 contains data for row 6

Store rows containing binary data as individual events = False

All rows are stored, but rows containing binary data are not stored as individual events. The FSA generates one event:

Event1 contains data for rows 1 through 6; no attachments

Specify FSA Server Properties

For each file scanning server, you can configure logging and performance settings. You can also configure retry attempts if an error occurs, and the number of DoD deletions.

1. Expand the scans branch .
2. Right-click a file scanning server and click Properties.

   The Server Properties dialog appears.
3. Specify server properties in the following tabs:

   Logging

   Specify the logging level, and the maxi,um number and size of log files.

   Performance

   Specify how long the FSA spends waiting and the number of worker threads.

   Error handling

   Configure the retry options. For example, you specify how many times CA DataMinder tries to analyze a scanned item if the first attempt fails.

   DoD Delete

   Specify the number of overwrites for DoD deletions.

FSA User Accounts

To create an FSA scanning job, you need to provide credentials for two Windows domain users:

FSA Job Setup User

The Job Setup User is the Windows account that you use to log on to the Administration console. The Administration console uses this account to connect to the scanning server when you create or manage scanning jobs using the FSA job definition wizard.

The Job Setup User must have write access to the \FSA\Jobs subfolder on the FSA host server. Find this subfolder in CA's folder in the Windows All Users profile on the machine hosting the FSA.

FSA Run As User

The Run As user is the account that a scanning job runs as. You specify the Run As user when you schedule a scanning job using the Job Definition wizard.

When choosing a Run As user, we recommend that you choose a bespoke account created for exclusive use by scanning jobs. This is because it is essential that nobody logs onto a scanned machine using the Run As account while a scheduled scan is running.

There are two types of FSA Run As user ('limited access' and 'full access users), reflecting their different purposes. The account requirements for the Run As user varying according to the purpose of the scanning job.

More information:

FSA Run As User (see page 98)

FSA Run As User

This is the account that a scanning job runs as. You specify the FSA Run As user when you schedule a scanning job using the Job Definition wizard or when you log on to Windows before running a scanning job from a command line.

Choosing the Run As user

Important! When a scheduled scanning job is running, it is essential that nobody logs onto the target machine using the same account as the FSA!

If a user and the FSA are logged on to the same machine, at the same time, and using the same Windows user account, this can adversely affect the scanning job. The job may terminate prematurely or it may even fail to respond to attempts to terminate it manually.

For this reason, you must be careful when choosing the Run As user for a scheduled scanning job. Specifically, if you want jobs to run as your FSA limited access user or FSA full access user, we recommend that these users are bespoke accounts created for exclusive use by the FSA. Do not choose a Run As user that corresponds to a real user account if there is any possibility that this user will be logged on to the target machine while a scheduled scanning job runs.

Avoid this situation! The classic mistake is when a network administrator schedules a scanning job and enters their own domain account as the Run As user (because they know that they have access to all the required scan locations). While performing an unrelated task, they subsequently log on to the target machine while the scan is in progress, so causing the scan to fail.

Types of Run As user

There are two types of FSA Run As user, reflecting their different purposes:

'Limited Access' FSA Run As User

You can use the FSA to test whether sensitive documents stored on your network are accessible to unauthorized users. To do this, you set up a scanning job to run as a user with limited access to sensitive network locations. This is your 'limited access FSA Run As user'. In effect, the limited access user is a proxy for your ordinary network users.

'Full Access' FSA Run As User

You can use the FSA to scan the content of files stored on your network to determine if sensitive information is stored in the correct location or to identify files or documents with unauthorized content. (Indeed, this is often regarded as the 'classic' use for the FSA.) To do this, the FSA must be able to access remote file systems and delete files when instructed to do so as a result of policy processing. Specifically, the FSA must run as a domain user with permission to delete and copy files on any machines that you want to scan. This user is your 'full access FSA Run As user'.

Requirements for Run As user

If you want to scan:

Microsoft Exchange Public Folders

When scanning Exchange public folders, the FSA Run As user requires:

- An Exchange mailbox. You can typically create a mailbox at the same time as you create a new user account in Active Directory.
- Read access to Exchange Public Folders. However, the full access user needs Read and Write access to be able to copy or delete Public Folder items.

The FSA also requires a default e-mail application compatible with Microsoft Exchange, such as Microsoft Outlook.

Microsoft SharePoint

When scanning a SharePoint site, the FSA Run As user must be a domain user with:

- Local administrator rights on the SharePoint host machine.
- Read access to the SharePoint site being scanned. However, the full access user will need Read and Write access.

For full details, see the *Stored Data Integration Guide*; search for 'FSA user accounts'.

Chapter 7: Event Auditing Setup

This section contains the following topics:

Overview (see page 101)
Audit Options (see page 102)
Suppress Automatic Auditing (see page 109)
About the Review Queue (see page 109)

Overview

Reviewers can use the CA DataMinder iConsole to update the audit trail of any captured or imported event (email, Web, file, or IM). Access to the audit features inthe iConsole is controlled by administrative privileges. These privileges enable CA DataMinder administrators to closely control the scope of a reviewer's authority.

Use the Administration console to set up and configure the iConsole auditing features.

More information:

Suppress Automatic Auditing (see page 109)
Set up Audit E-mail Templates (see page 108)

Audit Options

For reviewers to make full use of the iConsole event audit features, administrators must configure these features in the Administration console:

Audit fields

Field labels and list items in the iConsole Issue dialog are fully configurable, so administrators can customize the terminology and available options to meet your organization's requirements. For example, they can define multiple 'audit status' labels, 'actions taken' labels and other predefined comments. They can also specify additional, mandatory updates to the audit trail when a reviewer changes an event's audit status. For audit emails, administrators can also predefine recipient addresses and the email subject.

Audit buttons

Administrators can customize the behavior of audit buttons in the iConsole toolbar. These buttons allow reviewers to instantly change specific audit details from one value to another. For example, they can configure a button to automatically change the audit status of the currently selected events, or to change the 'Action Taken' from 'Reviewed' to 'Referred to Compliance Officer'. Up to ten separate buttons can be configured.

Note: If you reconfigure an audit buttons, the changes only become effective when a reviewer next logs into the iConsole. Reviewers currently logged on to the iConsole must log off and log back on before these changes become effective.

Audit email templates

Administrators can define templates for audit emails and make them available to reviewers in the iConsole (in the Compose Email dialog). These templates can include predefined recipient lists, plus predefined body and subject text to match your organization's terminology and requirements. Reviewers can use these templates, and change the predefined details if necessary, when composing audit emails.

Important! If these event auditing features are not fully configured in the Administration console, then event auditing will not be available in the iConsole. That is, reviewers will not be able to audit events in either console.

More information:

Set up Audit Field Labels (see page 103)
Populate Audit Field Lists (see page 104)
Set up Audit E-mail Templates (see page 108)
Overview (see page 101)

Set up Audit Field Labels

Organizations can tailor the audit fields so that the terminology used and the available options can be changed to meet their requirements. For example, administrators can define multiple 'audit status' labels, 'actions taken' labels and other comments. These appear as headings to the drop-down lists available in the Issue dialog in the iConsole.

1. In the Administration console, choose Tools, Audit Options.
2. In the General tab, click Modify to specify names for the Field 1, Field 2 and Field 3 tabs.

   Note: Field 1 is always used to define audit status information, but you can define a new name for it, if required. <Field 2> and <Field 3> can define other audit information.
3. You define the field items in the following tabs in the Audit Options dialog:
   - Field 1 - <Name>
   - Field 2 - <Name>
   - Field 3- <Name>

Note: If the audit fields are not fully configured in the Administration console, then event auditing will not be enabled in the iConsole. That is, reviewers will not be able to audit events in either console.

Populate Audit Field Lists

These are the list items available to reviewers in the Edit Issue dialog in the iConsole. <Field 1> always lists the available statuses for captured events being reviewed. That is, the type of audit status.

To define list items for all configurable audit fields in the iConsole

1. In the Administration console, choose Tools, Audit Options.
2. In the Audit Options dialog, go to the following tabs:

   Field 1 - <Name>

   Double-click an item to define up to 40 audit status names (see page 105), for example, Not reviewed or Approved. Audit status 0 and audit status 1 are special cases.

   Note: You can also specify further mandatory audit changes for any individual status change.

   Field 2 - <Name>

   Double-click an item or use the Modify button to define up to 40 <Field 2> items.

   Field 3 - <Name>

   Double-click an item or use the Modify button to define up to 40 <Field 3> items.

   Comment

   Use the Add, Remove and Modify buttons to create a list of comments, for example, Potential compliance violation or Satisfactory explanation provided by sender. This list of comments is also available to reviewers in the iConsole.

   Note: If your comment exceeds the maximum length for a comment (255 characters), it will be truncated.
3. Click OK to save your settings and return to the Options dialog.

Note: If the audit fields are not fully configured in the Administration console, then event auditing will not be enabled in the iConsole. That is, reviewers will not be able to audit events in either console.

More information:

Types of Audit Status (see page 105)
Specify Audit Field Dependencies (see page 106)
Specify Further Mandatory Audit Changes (see page 106)

Types of Audit Status

Audit Field 1 is always used to define audit status information. When you define the list items for Field 1, you can define up to 40 audit statuses and label them as required.

Audit status 0 and audit status 1 are special cases:

- Audit status 0 is the default status for unreviewed events. Newly captured or imported events are automatically assigned to audit status 0. Events with this status are yet to be reviewed and we recommended that you define audit status 0 as Not reviewed.
- Audit status 1 is the default status for reviewed events. By default in the iConsole, the audit button automatically advances the audit status from 0 to 1. If you intend to use this button with its default configuration, we recommend that you define audit status 1 as Approved.
- Audit status 2 through 39 are standard status types. You can change or delete their status names as required.

Note: If the audit status fields are not fully configured in the Administration console, then event auditing will not be enabled in the iConsole.

More information:

Populate Audit Field Lists (see page 104)
Set up Audit Field Labels (see page 103)

Specify Audit Field Dependencies

If necessary, you can configure which audit values are available for selection when a specific audit <Field 1> or <Field 2> value is selected. That is, you can configure dependencies between audit <Field 1> and <Field 2> values, and between audit <Field 2> and <Field 3> values.

For example, if Field 1 is 'Status' and Field 2 is 'Classified As', you can configure these audit field dependencies so that if a reviewer then uses the iConsole to set an issue status to 'Not Approved', they can only choose from a specific subset of 'Classified As' values.

To configure Field 1 and Field 2 dependencies

1. In the Administration console, choose Tools, Audit Options.
2. You set up audit dependencies in the following tabs:
   - Field 1 - <Name>
   - Field 2 - <Name>
3. In the Field 1 tab, select the value that you want to configure click Modify.
4. From the Available 'Field 2' Values list, select the Field 2 values you want to be available to reviewers when they select the current Field 1 value.
5. In the Field 2 tab, select the value that you want to configure click Modify.
6. From the Available 'Field 3' Values list, select the Field 3 values you want to be available to reviewers when they select the current Field 2 value.

Specify Further Mandatory Audit Changes

If necessary, you can force iConsole reviewers to add further details when changing an event's status. Specifically, you can specify that accompanying updates to <Field 2> and <Field 3> are mandatory. For example, if a reviewer changes an event's status to Actionable, you can specify that they must also update <Field 3>, which is typically used to specify any accompanying action taken.

To specify mandatory audit changes

1. In the Administration console, choose Tools, Audit Options.
2. Go to the Field 1 - <Name> tab.
3. Select the value that you want to configure and click Modify.
4. In the resulting dialog, go to the Other Audit Fields drop-down list and choose 'Must be completed'.
5. Click OK.

   Your changes will take effect with the next logon.

Set up the iConsole Audit Buttons

You can customize the behavior of the audit buttons in the iConsole toolbar, such as and .

These buttons allow reviewers to instantly change specific audit details from one value to another. For example, they can configure a button to automatically change the audit status of the currently selected events, or to change the 'Action Taken' from 'Reviewed' to 'Referred to Compliance Officer'. After a reviewer has audited an event using one of these buttons, the corresponding issue is added to the event's audit trail.

Important! iConsole reviewers cannot audit events until audit buttons have been configured in the Administration console.

Note: If you reconfigure an audit buttons, the changes only become effective when a reviewer next logs into the iConsole. Reviewers currently logged on to the iConsole must log off and log back on before these changes become effective.

To configure the iConsole audit buttons

You configure audit buttons in the Audit Options dialog.

1. In the Administration console, click Tools, Audit Options.
2. If you have not already done so, set up predefined values for the Status, Classified as, and Action/Resolution fields. You can also predefine audit comments.

   Details are in Populate Audit Field Lists (see page 104).
3. Go to the Tool Buttons tab.

   This tab lists the available audit buttons. For each audit button, its properties are shown as clickable hotspots.
4. Click the button property that you want to change:

   Single event audit or bulk event audit

   Choose whether the button is enabled for reviewing only single events, only search results, or both.

   Field 1 (typically 'Status')

   Select the audit status associated with this button. For example, you may want the button to change the audit status to Escalate.

   Field 2 (typically 'Classified as')

   Select the new classification that will be assigned to events when this button is clicked.

   Field 3 (typically 'Action/Resolution')

   Select the new action or resolution value that gets assigned to events when reviewers click this button.

Issue Name

(Optional) Type in the name of any new issue created when reviewers click this button.

The name is displayed in the Issues section of the iConsole Search Results screen.

Comment

(Optional) Type the comment that you want to add tot he audit trail when reviewers click this button.

Tooltip

Type in a name for the button. The name is displayed when the mouse pointer hovers over it in the toolbar.

Set up Audit E-mail Templates

CA DataMinder enables reviewers to forward events as e-mail attachments. For example, you can send an important event to a colleague for further assessment. In order to match an organization's terminology and requirements, administrators can define several e-mail templates for reviewers to choose from when they compose an audit e-mail in the iConsole.

To define e-mail templates in the Administration console

1. Choose Tools, Audit Options.
2. In the Audit Options dialog, go to the General tab, click Define Templates.
3. In the Audit Mail Templates dialog, use the Edit or Add buttons to modify an existing template, or create a new one. If you create a new template, CA DataMinder prompts you to give it a name.
4. In the Edit Template dialog, specify a default subject, the recipient e-mail address, and any body text you want to include.
5. These details are added to the e-mail automatically when a reviewer clicks Send Mail in the iConsole. If necessary, the reviewer can change these details fields or choose another template before sending the actual e-mail.
6. Click Save Template to close the dialog and then close the Audit Mail Templates dialog and the Options dialog.

More information:

Overview (see page 101)

Suppress Automatic Auditing

By default, CA DataMinder updates an event's audit trail each time the event is viewed in the Data Management console or iConsole. You can assign audit privileges to suppress this:

- Audit: Always suppress automatic auditing: If a reviewer has this privilege, they can view events without CA DataMinder adding a Viewed Event entry to the audit trail.
- Audit: Choose to suppress automatic auditing: If a reviewer has this privilege, they can choose whether to view events without adding a Viewed Event entry to the audit trail each time they open an event.

Note: If both privileges are set, Audit: Always suppress automatic auditing overrules Audit: Choose to suppress automatic auditing.

Both administrative privileges permit the reviewer to view events without updating the audit trail. Other audit activities, such as changing an event status or forwarding a copy of the event via e-mail will create an audit entry.

More information:

Overview (see page 101)

About the Review Queue

The Review Queue (RQ) feature enables to reviewers to generate lists of events that they need to review or audit.

RQ comprises an iConsole search and several reports:

Review Queue search

After RQ has been installed and configured on the CMS, any reviewer can run this search in the iConsole to retrieve all unreviewed events in their review queue. (Unreviewed events are assigned to reviewers based on their management groups.)

Review Queue reports

These provide administrators with technical information about RQ database searches, such as 'event selection rules' and summary event counts.

The required RQ database components are installed automatically when you install or upgrade a CMS. You can install the RQ search and reports from the CA DataMinder reports.msi installation package. For instructions on how to install and manage the Review Queue, see the Review Queue Guide. This is available to download from CA Technical Support: http://ca.com/support

More information:

Overview (see page 101)

Chapter 8: Logfiles

The Logfiles screen displays logfiles of all significant system events.

This section contains the following topics:

Overview (see page 111)
Log Types (see page 113)
Find Log Entries (see page 116)
View Log Files (see page 117)
Configure Log Files (see page 118)
Write to Windows Event Log (see page 119)
Write to a Syslog Server (see page 121)

Overview

CA DataMinder maintains logs for all product components to record significant activity or events.

Log file names

Log file names indicate the type of log, and incorporate the date and time when the file was created. For example, activity_200903170945.log is an Activity log created on 17 March 2009 09:45.

Where are log files saved?

Log files are typically stored locally in CA's \data\log subfolder of the Windows All Users profile, although there are exceptions (such as the PE hub log files).

The example below shows this location within a typical folder structure:

```
- All Users
  - Application Data
    - CA Technologies
      - CA DataMinder
        - data
          + FSA
          + log
          + PRC
+ Default User
+ srimmel
+ lsteele
+ fschaeffer
```

More information:

Log Types (see page 113)

Log Types

You can view the following types of log in the Administration console:

Note: Other CA DataMinder log types (such as policy engine hub logs) cannot be viewed in the Administration console. For details, see the Platform Deployment Guide; search for 'log files: types'.

Account Import logs

These are infrastructure-based logs. They record the outcome of any operations using Account Import. Log entries typically include changes to the user or machine hierarchy, such as the addition of new users, groups or client machines. Log File names take the format: ldap_<date>.log.

Activity logs

These are infrastructure-based logs. They record general activity by all machines. For example, each time users or machines log in or out, and each time policies are created or updated. Log File names take the format: activity_<date>.log.

You can also record user account changes in the User Administration log.

Content Services logs

These are infrastructure-based logs. They record the outcome of content indexing operations, including all significant connection and job events. Log File names take the format: index_job<n>_<date>.log.

Event Import logs

These logs are not infrastructure-based, but are viewable in the Administration console.

They record the outcome of Event Import operations, including details of all successful and unsuccessful events and any system errors (for example, when a user cannot be created). Log File names take the format:

`evtimport_<instance>_<date>.log`

Where <instance> identifies the service instance associated with the Event Import job.

File Scanning Agent logs

These logs are not infrastructure-based, but are viewable in the Administration console.

They record the outcome of FSA scanning jobs, such as details of replaced files, connections to the scan database, and when jobs started and completed. FSA log files are saved on the machine hosting the FSA. Log File names take the format: wgnfsa_<date>.log.

iConsole logs

These logs are not infrastructure-based, but are viewable in the Administration console.

They record the outcome of iConsole operations, including details of any errors. Log file names take the format: iconsole_<date>.log.

Policy Incident logs

These are infrastructure-based logs. They record the outcome of user policy processing. Each time a policy incident is replicated to the CMS, an entry is written to a log file. Log entries identify the associated user and include a URL to view the incident in the iConsole.

Log File names take the format: policyincident_<date>.log.

Replication logs

These are infrastructure-based logs. They record any database changes that were made on a remote machine and copied to the local machine. These typically include captured data objects, changes to a machine or user policy, and changes to user accounts and user groups. These changes are recorded in the replication log on each machine. Log File names take the format: repl_<date>.log.

System logs

These are infrastructure-based logs. They record any infrastructure errors that occur while the CA DataMinder infrastructure service is running. Under normal conditions, this log file is empty. Log File names take the format: stderr_<date>.log.

Note: Any errors detected when the infrastructure service starts up are written to the file wgninfra.out. Find this file in the same folder as the System log.

Tasks logs

These logs are not infrastructure-based, but are viewable in the Administration console. They record the outcome of jobs run using the WgnTask.exe utility. Log File names take the format:

```
task_<title>_<date>.log
```

Where <title> is an optional identifier based on the title parameter in the associated job definition document. For example, a task based on the Universal Extractor's XML metadata extractor may generate log files in this format:

```
task_Extracted XML metadata_200903170945.log
```

User Administration logs

These are infrastructure-based logs. They record any changes made to user accounts or groups. These typically include changes to user accounts and user groups. Log File names take the format: useradmin_<date>.log.

More information:

Logfiles (see page 111)
About Policy Incident Logs (see page 115)
Overview (see page 111)

About Policy Incident Logs

These logs are created on the CMS only. They record the outcome each time a user policy trigger fires. The log includes both event-level and trigger-level entries.

A key feature of these of log entries is that they include an event URL to display the incident in the iConsole. Administrators can use this URL to view the incident (for example, a captured e-mail) in the iConsole, plus any attachments and a summary of the policy that was applied.

Event-level messages

Only one of these messages is logged for each event, regardless of how many triggers the event causes to fire. They are structured as follows:

```
<Associated user>
<Message ID>
<User action>
<Policy outcome>
<Event severity>
<Machine name>
<Event ID>
<Event URL>
```

Where:

<Associated user>

Is the primary participant of an event, for example, the sender of an outgoing e-mail.

<Message ID>

Is a code that identifies the message type (event-level or trigger-level) and severity.

<User action>

Briefly describes what the user did (for example, 'The user sent an e-mail') or the event type (such as 'Scanned file') .

<Policy outcome>

Summarizes the outcome of policy processing. For example, CA DataMinder blocked the e-mail or warned the sender.

<Event severity>

Indicates which severity band the event is assigned to (Low, Medium or High).

<Machine name>

Indicates the source machine. For example, this could be the machine from which an e-mail was sent.

<Event ID>

Uniquely identifies a captured or imported event in the CMS database.

<Event URL>

Provides a URL to display the event in the iConsole. Users can browse to this URL to view the event in the iConsole.

Trigger-level messages

For each trigger that fires, a log message records these details:

```
<Associated user>
<Message ID>
<Trigger name>
<Event severity>
<Event ID>
<Event URL>
```

Where:

<Trigger name>

Identifies which policy trigger activated.

Other message details are the same as for error-level messages—see above.

More information:

Log Types (see page 113)

Find Log Entries

To quickly find a specific log entry, use the Find feature

1. Open the log you want in the Administration console.
2. Click or press Ctrl+F.
3. Enter the text in the Find dialog.

   You do not need to enter the whole word. You can search on the first few letters of any word, and you do not need to match the case.
4. You can quickly search the log to find other occurrences of this text:

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

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

More information:

Logfiles (see page 111)
View Log Files (see page 117)

View Log Files

By default, the Administration console lists logfiles on the local machine. But you can also view logfiles on remote machines.

To view local logfiles

1. Choose Manage, Logfiles or click .
2. Browse the available logfiles and choose the one you want to view:
3. indicates a closed logfile.
4. indicates the current logfile.

   Note: You can only view logfiles if you have been granted the View Logfile privilege.

To view remote logfiles

1. Choose Manage, Machine Administration or click .
2. Expand the machine hierarchy and select the machine you want.
3. Right-click and choose View Logfile.

More information:

Logfiles (see page 111)

Configure Log Files

Log files generated by the CA DataMinder infrastructure can be configured in the local machine policy. For some logs, you can also choose which types of event are logged.

Configuration for infrastructure-based log files

1. Edit the required machine policy.

   You can the common policy (see page 164) for client machines or gateways or the policy for an individual machine (see page 164).

2. In the Machine Policy Editor screen, go to the Infrastructure > Logging folder. Policy settings in this folder specify the maximum number and size of log files and whether log entries are copied to external logs.

   Further settings configure the individual log types. For example, you can specify which activities are recorded in the Activity log file. Likewise, for the Policy Incidents log you must specify the iConsole address that is incorporated into the event URL in each log message.

   For details about these policy settings, click Logging settings.

3. If required, you can configure CA DataMinder to send log messages to the Windows event log.

4. If required, you can configure CA DataMinder to send log messages to a Syslog server:

Configuration for non-infrastructure logs

Log files that are not created by the infrastructure (such as iConsole and Event Import logs) are configured using an alternative mechanism. For details, see the *Platform Deployment Guide*; search for 'log files, configuring'.

More information:

Logfiles (see page 111)
Edit a Policy (see page 164)
Edit Common Machine Policies (see page 164)
Logging Settings (see page 169)
Write to Windows Event Log (see page 119)
Write to a Syslog Server (see page 121)

Write to Windows Event Log

CA DataMinder can copy log entries to the local Windows Application log (accessible through the Windows Event Viewer). This enables you to use third party monitoring and alerting software such as Microsoft Operations Manager (MOM) to, for example, notify your administrators when a CA DataMinder error occurs by forwarding the error message to pagers or sending an e-mail alert.

To set up external logging to the local Windows Application log, you must edit the machine policy. You can set a default log level, and you can also specify a custom log level for individual logs:

Default log level

The Write to Windows Event Log setting determines which log messages are copied to the Windows Application log. Find this setting in the Infrastructure > Logging folder. More.

You can set this to 'None' so that no messages are copied, or you can choose 'Errors Only', 'Errors and Warnings', or 'All Messages'. But note that you can also specify a custom log level for each individual log; this overrides the default log level—see below.

Custom log level for individual logs

For each log maintained by the CA DataMinder infrastructure, a Log Detail setting lets you set a custom log level. This specifies which messages are copied to the Windows log and overrides the default log level. In each case, you can choose 'None', 'Errors Only', or 'Errors and Warnings'. You can also choose:

- 'Use Default' to use the default log level defined by the Write to Windows Event Log setting.
- 'All Messages'. Any message written to the CA DataMinder log is also copied to the Windows log.

Configure the machine policy

For infrastructure-maintained log files only.

To enable external logging to the Windows Application log

1. In the Machine Administration screen, select the machine you want and open the Machine Policy Editor.
2. Browse to the Infrastructure, Logging policy folder.
3. Set the Default Log Level: Edit the Write to Windows Event Log setting.
4. Set custom log levels for individual logs: Do the following:
   a. Browse to the Infrastructure, Logging, External Logging, Windows Event Log policy folder.
   b. Edit the Log Detail settings as required.

5. Click to save your policy changes.

More information:

Logfiles (see page 111)

Write to a Syslog Server

CA DataMinder can send log messages to Syslog servers such as CA Enterprise Log Manager or ArcSight. To enable this, you need to edit the local machine policy to specify the message format and log level and to identify your Syslog server.

You can specify up to three different Syslog servers in the local machine policy. That is, you can simultaneously copy CA DataMinder log messages to three different Syslog servers.

Note: This help topic uses the term 'Syslog server' to refer to the Syslog receiver, also commonly known as a syslogd or syslog daemon.

To set up external logging to a Syslog server, you must edit the machine policy. You can set a default log level, and you can also specify a custom log level for individual logs:

Default log level

The Write to Syslog Server setting determines which log messages are copied to a Syslog server. Find this setting in the Infrastructure > Logging folder. More.

You can set this to 'None' so that no messages are copied, or you can choose 'Errors Only', 'Errors and Warnings', or 'All Messages'. But note that you can also specify a custom log level for each individual log; this overrides the default log level—see below.

Custom log level for individual logs

For each log maintained by the CA DataMinder infrastructure, a Log Detail setting lets you set a custom log level. This specifies which messages are copied to a Syslog server and overrides the default log level. In each case, you can choose 'None', 'Errors Only', or 'Errors and Warnings'. You can also choose:

- 'Use Default' to use the default log level defined by the Write to Syslog Server setting.
- 'All Messages'. Any message written to the CA DataMinder log is also copied to the Syslog server.

Configure the machine policy

For infrastructure-maintained log files only.

To enable external logging to a Syslog server

1. In the Machine Administration screen, select the machine you want and open the Machine Policy Editor.
2. Browse to the Infrastructure, Logging policy folder.
3. Set the default log level: Edit the Write to Syslog Server setting.
4. Set custom log levels for individual logs: Do the following:

a. Browse to the Infrastructure, Logging, External Logging, Syslog n policy folders.

b. Edit the Log Detail settings as required.

5. Configure the Syslog integration: Still in the External Logging, Syslog n policy folder, edit the settings that specify the Syslog server, the server and client ports, and the message protocol, format and maximum length.

6. Click to save your policy changes.

More information:

Logfiles (see page 111)
External Logging Settings (see page 173)

Chapter 9: Machine Administration

The Machine Administration screen is where you manage accounts for the CMS, gateway servers, and endpoint computers. Use this screen to manage machine accounts and view the current status of each CA DataMinder server or computer. You can also launch the Machine Policy screen directly from this screen.

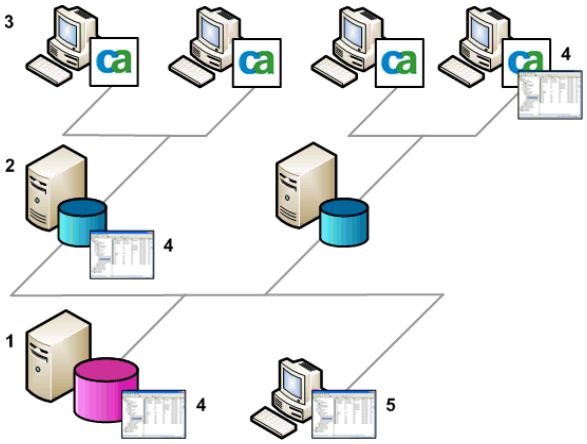
This section contains the following topics:

Overview (see page 124)
Machine Types (see page 125)
Managing Machine Accounts (see page 125)
Replication (see page 129)
Infrastructure (see page 133)
Editing Machine Policies (see page 135)
File Scans (see page 135)
Disabling E-mail and Browser Integration - Machine Administration (see page 136)
Monitoring Free Disk Space (see page 137)
Suspended Machines (see page 139)
Data Encryption (see page 142)
Data Compression (see page 146)
Event Purging (see page 146)
Diagnostics (see page 156)

Overview

CA DataMinder machines are organized into hierarchical branches, with the CMS as the top level server. Below the CMS, each branch of the hierarchy is managed by a gateway. Each gateway serves multiple endpoint computers. This type of distributed deployment provides resilience, network load balancing, and allows you to quickly and selectively roll out machine policies across your organization.

Note: You can install CA DataMinder consoles on any computer that can connect to the CMS.



1. CMS
2. Gateway servers
3. Endpoint computers
4. Consoles on CA DataMinder computers
5. Console-only computer

More information:

Machine Types (see page 125)

Machine Types

CA DataMinder installations comprise three types of machine: a CMS, gateways and client machines.

CMS

This is the central database for all your CA DataMinder installation. This database contains the policies for all your users and machines, plus all captured events.

Gateways

Gateways are intermediate servers, providing data-routing services between the CMS and client machines (see below). Each gateway can serve multiple client machines or even multiple child gateways. Gateways enable you to organize your CA DataMinder machines hierarchically in order to optimize network performance or selectively apply machine policies.

Client machines

These are the machines used by ordinary users. Each has its own machine policy held in a local database. This database also contains policy details and captured data associated with the current user.

Note: Captured data is periodically uploaded to the parent server.

Utility machines

These are host machines for CA DataMinder Content Proxy servers and iConsole application servers. Utility machines enable you to run these components without overloading your existing CA DataMinder servers.

More information:

Overview (see page 124)

Managing Machine Accounts

More information:

Add New Machines (see page 126)
Move Machines (see page 127)
Delete Machines (see page 127)
Rename Machines (see page 128)
Export the Machine Hierarchy (see page 128)
Import or Reparent Machines (see page 129)

Add New Machines

You can connect a new machine to the CMS or a gateway even if it does not yet have the CA DataMinder infrastructure installed. There are three ways to add new machines:

New client machines are added automatically

In the CMS machine policy, you can configure the Account Handling for New Client Machines setting to automatically create a new account for any client machine not registered with the CMS. When the CA DataMinder infrastructure next starts on that machine, a new account is created automatically and added to the CA DataMinder machine hierarchy.

Important! CA DataMinder cannot automatically create accounts for machines whose names contain Far Eastern characters.

Administrators add new machines

To manually add new client machines or gateways

1. Choose Manage > Machine Administration or click .
2. Select the CMS or an existing gateway . This will be the parent server for the new machine.
3. Choose Edit, New Machine or click .
4. In the Assign Machine dialog:
   - Enter the computer name or click Browse to search your network.
   - Specify whether the new machine is a Gateway or Client.

Import machine accounts

You can also import machine details from an external source using Account Import.

More information:

Managing Machine Accounts (see page 125)
Import or Reparent Machines (see page 129)

Move Machines

If necessary, you can reorganize the machine hierarchy. For example, to optimize load-balancing purposes you may want to move a client machine to a different gateway.

To manually move a machine

1. Choose Manage, Machine Administration or click .
2. Select the client machine or gateway you want to move.
3. Right-click and choose Move Item.
4. In the Move Item dialog, select the target parent server (either the CMS or a gateway).

Reparent multiple machines simultaneously

To do this, use the Account Import wizard. You specify the individual moves in a CSV file.

More information:

Managing Machine Accounts (see page 125)
Import or Reparent Machines (see page 129)

Delete Machines

To delete a machine

1. Choose Manage, Machine Administration or click .
2. Select the machine (or) you want to delete.
3. Right-click and choose Delete or click .
4. Select the client machine or gateway you want to delete.

More information:

Managing Machine Accounts (see page 125)

Rename Machines

CMS and gateways

Important! We strongly recommend that you do not rename the CMS or gateway servers.

Renaming the CMS or a gateway can cause severe communication problems between the server and its child machines. This is due to the authentication mechanism used by CA DataMinder machines to ensure data security.

Client machines

You can rename client machines, but be aware that CA DataMinder handles the renamed client as though it were a new machine. That is, the renamed machine is given a new account and inherits the common client policy (the default policy for new client machines).

If the local machine policy previously contained customized settings, these will be lost when the client is renamed. You will need to re-configure these settings in the policy for the new machine account.

More information:

Managing Machine Accounts (see page 125)

Export the Machine Hierarchy

You can export any branch of the machine hierarchy to a command file compatible with the Account Import wizard.

1. Choose Manage, Machine Administration or click .
2. Right-click the CMS or a gateway and choose Export Hierarchy to File.
3. In the resulting dialog, specify:
   - The command file name and location.
   - Which machine types to export (gateways, or client and utility machines).

   Note: Command files are configuration files containing CA DataMinder machine import commands. We recommend that you do not re-import the exported machine hierarchy back onto your working CMS.

More information:

Managing Machine Accounts (see page 125)

Import or Reparent Machines

To simplify mass deployments, you can bulk create new machine accounts and pre-assign client machines to parent servers in advance of the CA DataMinder rollout. This enables you to deploy multiple client machines using a single source image (which identifies a single parent server) whilst ensuring that each client machine automatically connects to its 'correct' parent server immediately after installation. You can also bulk move (or reparent) existing client machines and gateways to new parent servers.

To bulk create new accounts, you import the gateway and client machine details from a command file. You can do this using the Account Import wizard (launched from the Administration console; choose Tools > Account Import Wizard) or you can run a command line import operation. Command files for machine import operations are briefly described below.

Command Files

When you import a command file containing machine details, each record in the file must conform to the format required by Account Import. Each machine record must begin on a new line with a variable that defines the type of operation.

For example, the commands below create a new gateway, GW-MILAN, parented to CMS-HARDY, and a new client machine, UNI-TAYLOR, parented to GW-MILAN. The final command moves an existing client machine, UNI-ROBSON, to the new gateway:

```
newgateway,GW-MILAN,CMS-HARDY
newclient,UNI-TAYLOR,GW-MILAN
moveclient,UNI-ROBSON,GW-MILAN
```

Note: For full details about machine import operations, see the *Platform Deployment Guide*; search for 'Account Import'.

More information:

Managing Machine Accounts (see page 125)

Replication

More information:

Replicate CMS Changes to Client Machines (see page 130)
Replicate Captured Data to Parent Servers (see page 130)
Replication Notification Periods (see page 131)
Disable Replication (see page 132)
Replication Over Slow Network Connections (see page 133)
Replication Failures (see page 133)

Replicate CMS Changes to Client Machines

The CMS database holds policy details for each CA DataMinder user and machine, and administration details for each user, user group and machine. Any database changes are replicated automatically to child machines. The replication frequency is determined by the CMS machine policy. But you can request immediate replication. This is useful where CA DataMinder runs on networks using a slow CMS-to-child replication interval. To do this, choose Tools > Replicate changes to clients.

Note: You can also request warnings before you replicate changes. Choose Tools, Options and go to the General tab. Then, when you next replicate changes, CA DataMinder asks you to confirm the replication.

More information:

Replicate Captured Data to Parent Servers (see page 130)
Replication Notification Periods (see page 131)
Disable Replication (see page 132)

Replicate Captured Data to Parent Servers

Note: We use the term 'captured events' to refer to e-mail, Web and IM events captured directly by a CA DataMinder client or server agent, or events imported into CA DataMinder by the Event Import utility.

Each client machine and gateway server manages a database of captured events. For client machines, these are typically events captured locally; for gateway servers, these are usually events imported from an external source or events replicated up to the gateway from a child machine. In all cases, the local machine policy determines how often these events are replicated up to the CMS.

More information:

Replication Settings (see page 168)
Replication Notification Periods (see page 131)
Disable Replication (see page 132)
Replication Over Slow Network Connections (see page 133)
Replication Failures (see page 133)

Replication Notification Periods

Notification periods

All data replication across a CA DataMinder installation is driven by notification messages:

Captured data

Newly captured events are replicated as soon as possible from client machines to the CMS. The Captured Data Notification Period in the machine policy determines how often a client machine sends notification that it has captured new data. When the CMS receives this notification, it transfers the captured data from the client to the CMS and the client stops sending notifications.

Infrastructure data

The Infrastructure Notification Period in the machine policy determines how often client machines and the CMS notify each other of new infrastructure changes such as policy edits or user account updates. When the recipient machine receives this notification, it determines if it needs the update; if so, it requests the details. As soon as the recipient machine has processed the notification, the sender machine stops sending notifications.

More information:

Disable Replication (see page 132)

Disable Replication

If required, you can disable replication to and from individual machines. For example, you may want to temporarily stop the CMS sending policy change notifications to all CA DataMinder machines. To disable replication, you can either suspend a machine or server, or you can set the replication period to zero.

Suspend a machine

When a CA DataMinder machine is manually suspended, it can neither send or receive replicated data. For client machines, this means they can neither replicate captured data to their parent server or receive policy changes from the CMS.

Note: If a machine is suspended automatically (for example, because of a critical shortage of free disk space), under certain circumstances events captured locally before the suspension are still replicated up to the parent server.

Set the notification period to zero

You need to edit the policy for the machine that you want to stop replicating data. In the Replication folder of the machine policy, set the Captured Data Notification Period and Infrastructure Notification Period settings to zero in order to separately disable the outward replication of captured data and infrastructure changes. Note that the machine will still be able to receive replicated data.

This approach is also the quickest way to turn off all replication across the CA DataMinder enterprise. First, set the notification periods to zero for the common gateway policy and the common client policy. Then do the same for the CMS machine policy.

Note: Be aware that this approach will generate extra network traffic as the policy changes need to be transmitted around the enterprise.

More information:

Overview (see page 140)
Replication Notification Periods (see page 131)
Edit Common Machine Policies (see page 164)
Replication Failures (see page 133)

Replication Over Slow Network Connections

If there is a very slow connection between a client machine and its parent server, for example over a WAN, you can turn off replication. This primarily affects laptop users.

To turn off replication

1. In the Machine Policy Editor, browse the policy folders to the Replication folder.
2. Set the Replicate Captured Data on Slow Links setting to False.

Remember, you must periodically replicate any captured data that accumulates on the laptop. This requires regular (albeit temporary) policy changes to ensure that replication occurs. Alternatively, the laptop must make regular connections to its parent server over a LAN. For example, this could happen whenever the laptop user visits the office.

More information:

Replication Failures (see page 133)
Disable Replication (see page 132)

Replication Failures

If a parent server is unable to store a replicated event for any reason, it reports the failure back to the child machine, which writes an entry for the 'failed' event to the replication holding cache. For details, see the *Platform Deployment Guide*; search for 'holding cache'.

More information:

Replicate Captured Data to Parent Servers (see page 130)
Disable Replication (see page 132)

Infrastructure

More information:

Overview (see page 134)
Stop or Restart the Infrastructure without Rebooting (see page 134)
Run the Infrastructure as a Named User (see page 135)

Overview

Each CA DataMinder machine has an infrastructure—a collection of software components—that enables it to operate, communicate with other CA DataMinder machines, and protect confidential data. Settings in the local machine policy control the infrastructure:

- **Security** settings control whether CA DataMinder encrypts network data transfers and records in the local database, and whether logon credentials for CA DataMinder users are cached.
- **Data Management** settings cover data compression, data file block sizes, event purging, and free disk space handling.
  - When free disk space falls to critical levels, the infrastructure is suspended.
  - We strongly recommend that you set up a purging strategy as soon as possible after installation.
- **Replication** settings determine how often the local machine notifies its parent server of newly captured data or local infrastructure changes. These notifications act as triggers for data replication.
- **Logging** settings control which infrastructure operations are logged. You specify which operations are logged and the maximum size of log files.

More information:

Monitoring Free Disk Space Overview (see page 138)
Overview (see page 147)
Infrastructure Settings (see page 166)

Stop or Restart the Infrastructure without Rebooting

You can manually stop and restart the infrastructure using the wgninfra service. Run the following commands:

To stop the infrastructure

```
net stop wgninfra
```

To restart the infrastructure

```
net start wgninfra
```

Note: For further infrastructure information, please refer to the *Platform Deployment Guide*.

Run the Infrastructure as a Named User

When installing a CA DataMinder server or client machine, you must specify a logon account for the infrastructure. This defaults to LocalSystem, but if required you can specify a named user account. There are various conditions where when you may need to do this. Specifically, when installing:

- **A CMS or gateway,** if you specify a remote \Data folder then the local infrastructure must log on as a domain user with administrative rights to read and write to the remote folder.
- **The Remote Data Manager (RDM)**, the infrastructure must log on as a named user account. Also, this account must have the 'Log on a serivice' security privilege and permissions to retrieve data from an EAS archive. See the *Archive Integration Guide* for details; search for 'RDM'.

Editing Machine Policies

A machine policy contains settings that govern how CA DataMinder computers manage their database of captured events.

More information:

Edit Common Machine Policies (see page 164)
Infrastructure Settings (see page 166)
Policy Engine Settings (see page 178)
Client File System Agent Settings (see page 180)
Central Management Server Settings (see page 188)

File Scans

You can use the File Scanning Agent (FSA) and Client File System Agent to run file scans. To configure:

- **CFSA file scans**, you must edit settings in the machine policy. Specifically, you need to edit settings in the Client File System Agent, Data At Rest Protection policy folder.
- **FSA file scans**, you use the Job Definition wizard in the Administration console.

More information:

Client File System Agent Settings (see page 180)

Disabling E-mail and Browser Integration - Machine Administration

If required, you can disable e-mail and browser integration when you install CA DataMinder. You can also specify that integration is disabled if, for any reason, the CA DataMinder infrastructure fails to start.

Responding to an infrastructure failure

The 'Infrastructure Failure' setting in the user policy 'System Settings' folder controls how CA DataMinder responds if the infrastructure fails to start. In particular, you can use this setting to disable CA DataMinder integration with all browser and e-mail applications.

Installing with msiexec.exe

When installing CA DataMinder using deployment methods based on msiexec.exe, you can disable browser integration for Windows Explorer and Outlook. In practical terms, this means that if a user surfs the Web using Windows Explorer or Outlook as a browser, CA DataMinder does not monitor this activity. For more information on msiexec.exe parameters supported by CA DataMinder, refer to the *Platform Deployment Guide*; search for 'msiexec.exe, general'.

Note: Integration with Internet Explorer and email integration with Microsoft Outlook are not affected. CA DataMinder continues to monitor web activity in Internet Explorer and email activity in Outlook as normal.

Editing the user policy

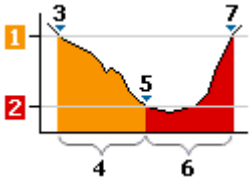
E-mail and browser integration can also be permanently disabled for individual users, or disabled for specific capture or control triggers, by editing their user policy.

Monitoring Free Disk Space

Settings in the machine policy let you monitor levels of free disk space on CA DataMinder machines and suspend the CA DataMinder infrastructure when free disk space falls below a critical level. Find these settings in the Infrastructure > Data Management folder.

For each CA DataMinder machine, these policy settings monitor free disk space on the drive hosting the Data folder (this folder, which may be remote, contains configuration data and captured data for the local CA DataMinder installation).

You can specify disk space warning and error levels, and how often free disk space is checked. If free space falls below the warning level, warnings are written to the Audit logfile. If it then falls below the error level, the CA DataMinder infrastructure is suspended. Note that the infrastructure restarts automatically when free disk space recovers to the warning level.



Changing levels of free disk space

1. Warning level.
2. Error level.
3. Free disk space falls below the Warning level.
4. During this period, warnings are added to the logfile.
5. Free disk space falls below the Error level.
6. During this period, the CA DataMinder infrastructure is suspended.
7. Free disk space recovers above the Warning level and the CA DataMinder infrastructure resumes automatically.

More information:

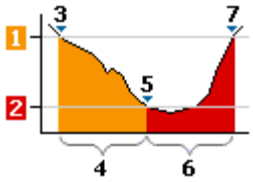
Monitoring Free Disk Space Overview (see page 138)
Disk Space Policy Settings (see page 139)

Monitoring Free Disk Space Overview

Settings in the machine policy let you monitor levels of free disk space on CA DataMinder machines and suspend the CA DataMinder infrastructure when free disk space falls below a critical level. Find these settings in the Infrastructure > Data Management folder.

For each CA DataMinder machine, these policy settings monitor free disk space on the drive hosting the Data folder (this folder, which may be remote, contains configuration data and captured data for the local CA DataMinder installation).

You can specify disk space warning and error levels, and how often free disk space is checked. If free space falls below the warning level, warnings are written to the Audit logfile. If it then falls below the error level, the CA DataMinder infrastructure is suspended. Note that the infrastructure restarts automatically when free disk space recovers to the warning level.



Changing levels of free disk space

1. Warning level.
2. Error level.
3. Free disk space falls below the Warning level.
4. During this period, warnings are added to the logfile.
5. Free disk space falls below the Error level.
6. During this period, the CA DataMinder infrastructure is suspended.
7. Free disk space recovers above the Warning level and the CA DataMinder infrastructure resumes automatically.

More information:

Disk Space Policy Settings (see page 139)

Disk Space Policy Settings

Each machine policy contains three key disk space settings. Find these in Infrastructure, Data Management folder:

Note: These policy settings monitor free disk space on the drive hosting the Data folder (this folder, which may be remote, contains configuration data and captured data for the local CA DataMinder installation).

Disk space check interval

You must determine how often free disk space is checked. If you set this interval to zero minutes, free disk space is never checked.

Note: On the CMS and gateway servers, we strongly recommend you set this frequency to one minute.

Disk space warning level

When free disk space falls below this level, CA DataMinder adds a warning to the Activity logfile. The default warning level is 25 MB. If free disk space continues to fall, further warnings are added to the logfile until eventually free space falls to the error level and the CA DataMinder infrastructure is suspended. Up to 10 warnings are issued, with a minimum fall in free disk space of 1 MB between each warning.

The warning level (not the error level) also represents the 'safe' level at which the infrastructure automatically restarts following a suspension and subsequent recovery in free disk space.

Note: For the CMS and gateway servers, we strongly recommend you set this level to 250 MB.

Disk space error level

When free disk space falls below this level, the CA DataMinder infrastructure is suspended. The default value is 5 MB. Following a suspension, the infrastructure automatically restarts when free disk space recovers to the warning level (not the error level).

Note: For the CMS and gateway servers, we strongly recommend you set this level to 50 MB.

More information:

Monitoring Free Disk Space Overview (see page 138)

Suspended Machines

More information:

Overview (see page 140)
What Operations are Still Available on Suspended Machines? (see page 141)
Suspend or Resume a Machine (see page 142)

Overview

Suspended machines overview

When a CMS, gateway or client machine is suspended, all replication and notification activity ceases. That is, the machine is unable to receive data such as policy updates or newly captured data. Suspended gateways and client machines also stop sending notifications of newly captured data to their parent server.

Automatic suspensions

CA DataMinder machines are suspended automatically if:

- Free disk space falls below the Error Level. This level is defined in the Infrastructure > Data Management folder of the machine policy.
- Database problems arise. For example, CA DataMinder suspends a machine if there is a communication failure with the local database, or if the local database becomes full (that is, it fills its allocated space quota).
- A disk failure occurs. If a parent server is unable to replicate data because of a disk failure on a child machine, CA DataMinder suspends the child machine.
- The replication holding cache becomes full. Events that fail to replicate successfully are stored in a holding cache. If the cache's maximum event limit is exceeded, CA DataMinder suspends the child machine. For details, see the Platform Deployment Guide; search for 'holding cache'.

Manual suspensions

You can also manually suspend a machine. You may want to do this to carry out maintenance. For example, a scheduled backup will complete faster on a suspended CMS. This is because data transfers from gateways and client machines to a suspended CMS are discontinued until the CMS resumes data processing.

Note: To suspend or resume CA DataMinder machines, your user account must have the Edit Machine Hierarchy administrative privilege.

More information:

Disk Space Policy Settings (see page 139)

What Operations are Still Available on Suspended Machines?

Certain CA DataMinder operations continue or remain available on a suspended client machine:

Replication

If a client machine is suspended automatically due to a lack of free disk space or because the local CA DataMinder database is full, data captured on the client machine before the suspension occurred is still replicated up to the parent server.

Note: If a client machine is suspended for other reasons (for example, a manual suspension), captured data is not replicated up to the parent server until the client machine resumes.

Policy

You can still edit user and machine policies on suspended machines if the machine was suspended manually (see below). For example, even if you suspended the CMS you can still amend the policy of any machine or any user in your management group.

Note: These policy changes are not replicated to the relevant client machine until the CMS resumes.

Control triggers and actions

On a suspended client machine, control triggers and actions continue to operate but the resulting control events are not saved. For example, you cannot search for blockings or warnings that occurred while a client machine was suspended.

Note: Capture triggers do not operate on a suspended machine.

More information:

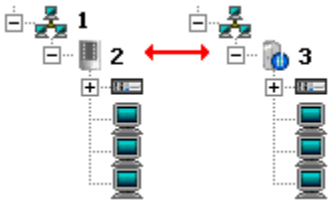
Overview (see page 140)

Suspend or Resume a Machine

You must have the 'Edit Machine Hierarchy' administrative privilege to be able to suspend or resume CA DataMinder machines,

To suspend or resume a CMS

1. Expand the Machine Administration branch (**1**) and select the CMS.
2. Do one of the following:
   - Right-click an active CMS (**2**) and choose Suspend.
   - Right-click a suspended CMS (**3**) and choose Resume.



To suspend or resume a gateway or client machine

1. Expand the Machine Administration branch and select the gateway or client you want.
2. Right-click the machine and choose Machine State.
3. In the resulting dialog, click Suspend or Resume.

More information:

Overview (see page 140)

Data Encryption

Encrypt Replicated Data

Data encryption is controlled by settings in the machine policy. If required, you can encrypt all data sent across the network between CA DataMinder machines.

To encrypt data

1. In the Machine Policy Editor, browse to the Security folder.
2. Edit the Communications Encryption setting. You can choose from low, medium or high encryption.

More information:

Security Settings (see page 166)
Encrypt Stored Data (see page 143)

Encrypt Stored Data

Encrypting your stored data prevents intruders from accessing sensitive information by reading the blob files directly. This is especially important on the CMS where the blob files contain captured e-mail and Web data for the whole enterprise.

The data store on each CA DataMinder machine incorporates 'blob' (Binary Large Object) files, containing policy data and, on the CMS and gateways, captured Web and e-mail data (on client machines, blob files containing captured data are not encrypted).

Machine policy settings enable you to optionally encrypt these blob files with a local encryption key. You can also manually change the master key used to encrypt the local encryption keys.

More information:

Encryption Key Changes (see page 144)
Set the Encryption Key Change Thresholds (see page 144)
Change the Master Encryption Key (see page 145)

Encryption Key Changes

Each CA DataMinder machine has a unique encryption key that is used when writing blob files to disk. Further settings in the machine policy determine how often the local key is changed.

By default, regular key changes occur automatically to reduce your exposure to security risk. Limiting the volume of data encrypted with a single key means it is harder for an intruder to crack the key. It also means that in the unlikely event they succeed, they will only gain access to a small part of your total data store. Note that superseded keys are retained so that older files can still be read.

In normal situations, it is not necessary to edit these policy settings because the default values have been carefully chosen. But if you need to strengthen security on the CMS (or a gateway), you can modify two key replacement thresholds:

Time interval

The key is changed after the specified number of days. For example, you can specify a key change every seven days.

Volume of data

The key is changed after it has encrypted the specified volume of data. For example, you can specify a key change after every 1 GB of captured data. (On the CMS, this threshold measures how much data has been captured and encrypted across your entire CA DataMinder installation.)

These thresholds operate in parallel. The encryption key is changed as soon as either threshold is exceeded, and both threshold counters are immediately reset to zero.

More information:

Encrypt Stored Data (see page 143)

Set the Encryption Key Change Thresholds

To set the key change thresholds on your CMS or a gateway server

1. Expand the Machine Administration branch .
2. Right-click the machine you want and choose Edit Policy.
3. In the Machine Policy Editor, browse to the Security folder.
4. Edit the two Data Store Encryption Key Change settings. The 'Volume' threshold is defined in megabytes; the 'Interval' threshold is defined in days.
5. Save the machine policy.

Note: It is unlikely you will need to edit these settings on your client machines. Encrypted blob files on these machines only contain policy data.

More information:

Encrypt Stored Data (see page 143)

Change the Master Encryption Key

On each CA DataMinder machine, the keys used to encrypt stored data (the blob file keys) are themselves encrypted with a master key. For maximum data security, CA DataMinder allows you to manually change this master key.

Clearly, changing the master encryption key, especially on the CMS, is an extremely sensitive task. For this reason, the key change process has been rigorously engineered to eliminate the risk of data loss arising from an unrecoverable blob file encryption key. In particular, CA DataMinder:

- Prevents the automatic creation of new blob file encryption keys while the master key change is underway or when a machine is starting up.
- Scrupulously records each stage of the process in key change recovery files to enable automatic rollback if the key change fails.

CA DataMinder provides a command line method for manually changing the master encryption key. The command syntax is:

```
wgninfra -exec  wigan/infrastruct/database/KeyServices ManageKeys -m
```

Where:

wigan/infrastruct/database/KeyServices

Is the Java Class path. You must type this path exactly as shown here.

ManageKeys

Identifies the command as an encryption key operation.

-m

Specifies that the operation applies to the local master key.

More information:

Encrypt Stored Data (see page 143)

Data Compression

Machine policy settings allow you to compress data stored on the local server and data replicated between CA DataMinder machines.

Event Purging

More information:

Overview (see page 147)
Purging Strategies (see page 148)
What Data is Purged? (see page 149)
Minimum Retention Period (see page 150)
Purge SPs (see page 151)
Configure Purges in the Machine Policy (see page 152)
Selective Trigger-Based Purging (see page 153)
Turn off Purging (see page 154)
Purge Policy Settings (see page 155)

Overview

Note: This topic and the linked topics below refer to scheduled event purges driven by the CA DataMinder infrastructure. But for Oracle databases, CA DataMinder also supports partition-based purging. For details, see the Database guide; search for 'partition-based purging'.

After installing CA DataMinder, you need to turn on database purging to periodically remove events from CA DataMinder databases. By default, purging is turned off on CA DataMinder machines, but we recommend that you enable purging, especially on your gateways and client machines.

You need a separate purging strategy for your CMS, which holds captured data for your entire organization, and one or more strategies for your gateways and client machines. To implement these strategies, you need to configure the CMS, common gateway and common client machine policies.

CA DataMinder events become eligible for purging when their minimum retention period expires. Each event purge removes eligible database records plus any associated blob (binary large object) files.

Settings in the machine policy control how often events are purged from the local machine. Other settings provide further control over purge operations. For example, you can choose to suspend the CA DataMinder infrastructure during purge operations or you can specify a purging timeout.

More information:

Event Purging (see page 146)

Purging Strategies

Event purging strategies

After installing CA DataMinder, you need to turn on database purging to periodically remove events from CA DataMinder databases. You need a separate purging strategy for your CMS, which holds event data for your entire organization, and one or more strategies for your gateways and client machines. To implement these strategies, you need to configure the CMS, common gateway and common client machine policies.

CMS purges

Compliance-seeking organizations need to implement an event purging strategy that meets regulatory requirements on the storage and retention of historical communications. Typically, this strategy requires scheduled purges. These run at regular intervals and are configurable in the CMS machine policy.

If you set up scheduled purging, you must also specify the minimum retention period for captured items before they become eligible for purging. For example, you may be required to retain e-mails for a minimum of three years.

Gateway and client machine purges

Events stored in the local database of a gateway or client machine are eventually replicated up to the parent server and ultimately to the CMS. The main reason for event purging on gateways and client machines is to prevent free disk space falling to dangerously low levels on these machines, with the attendant risk of the CA DataMinder infrastructure being suspended.

The simplest strategy is to implement purging after replication. Under this strategy, individual items of captured data are automatically excluded from purges until they have been replicated to the parent server. Only items that have already been replicated can become eligible for purging.

To roll out a purging strategy across all of your gateways and client machines, simply edit the Common Gateway Policy and Common Client Policy. If required, you can still specify a custom purge strategy for individual machines by editing their machine policy directly.

Partition-based purges

(Applicable to Oracle databases only)

The CA DataMinder database schema also includes support for Oracle database partitioning based on event time stamps, and for partition-based purging. For full details, see the Database guide; search for 'partition-based purging'.

More information:

Event Purging (see page 146)
Minimum Retention Period (see page 150)
Overview (see page 140)
Configure Purges in the Machine Policy (see page 152)

What Data is Purged?

Each purge removes eligible database records plus any corresponding blob (binary large object) files, if the blob files are stored locally. This is because each CA DataMinder event comprises metadata, written to the local CA DataMinder database, and a blob (Binary Large Object) file, saved on physical media.

- **The database record** contains the event metadata. For example, database fields specify an e-mail delivery date, 'envelope' details, what policy triggers were applied, and so on.
- **The blob file** contains the e-mail content and any attachments, or the Web page plus any uploaded files, stored in CA DataMinder format. The blob file is written to disk, saved in the \Data folder.

More information:

Event Purging (see page 146)

Minimum Retention Period

CA DataMinder events become eligible for purging from the CMS when their minimum retention period expires. The retention period is measured in whole days, from midnight to midnight. For example, a 1000 day retention period implies that captured events must be retained in the CA DataMinder database for at least one thousand whole days before they can be purged. An event's eligibility for purging therefore depends on its age. For:

- **Captured e-mails, files or Web pages**, their age is calculated from the time the trigger activated.
- **Imported e-mails**, the age is determined by the EMail.EventDateFromEMail parameter. This specifies whether the email capture date is set from the date in the e-mail itself or the date when it was imported. This parameter is described in the *Archive Integration Guide*; search for 'parameters: Event Import'.

Overriding the default retention period

CA DataMinder permits reviewers and policy administrators to override the default minimum retention period. For example:

- A reviewer may need to put an unauthorized e-mail on litigation hold. They can do this in the Review dialog of the Data Management console by overriding the expiry date of that e-mail's retention period. For example, they can specify that the retention period never expires.
- Policy administrators can set a custom retention period for all events captured by a specific trigger. For example, they may want to retain events captured by an Application Monitor trigger for one month only, but retain events captured by an e-mail trigger for three years.

More information:

Event Purging (see page 146)
Selective Trigger-Based Purging (see page 153)

Purge SPs

For both SQL Server and Oracle databases, CA DataMinder supports stored procedures (SPs). Public SPs, supplied with CA DataMinder, provide default purging functionality and can be overridden your own custom SPs, if required.

When the CA DataMinder infrastructure runs a database purge, it invokes the required public or custom purge SPs. Before a purge runs, the infrastructure also checks for any pre-purge SPs; when the purge completes or terminates, it checks for any post-purge SPs.

For full details, see the *Database Guide*; search for 'SPs'.

More information:

Event Purging (see page 146)

Configure Purges in the Machine Policy

To implement database purging, you need to configure the common gateway and common client machine policies

1. In the Administration Console, expand the Machine Administration branch .
2. To configure event purging for:
   - **The CMS**, right-click the CMS and choose Edit Policy.
   - **All gateways**, right-click the CMS and choose Edit Common Gateway Policy.
   - **All client machines**, right-click the CMS and choose Edit Common Client Policy.
   - **A specific machine**, right-click the machine and choose Edit Policy.
3. In the Machine Policy Editor, browse to the Data Management folder.
4. Set the purge frequency: You can configure purges to run immediately after the data has been replicated, or you can schedule purges to run at regular intervals.
   - **Scheduled purges:** To schedule regular purges, set Purge Events on Replication? to False (clear the check box). Then configure the policy settings for the minimum retention period and purge frequency and time.
   - **Purging after replication**: Set Purge Events on Replication? to True (select the check box). This purges your database as soon as captured or imported data has been replicated to the parent server. No further policy changes are required. This setting is ignored on CMSs; it is intended for use only with gateways and client machines.
5. **Configure purge performance:** Other settings in the Data Management folder provide further control over purge operations. For example, you can choose to suspend the CA DataMinder infrastructure during purge operations or you can specify a purging timeout.
6. Save the policy. Database purging is turned on as soon as the new settings replicate to the target CA DataMinder machines.

More information:

Event Purging (see page 146)
Purge Policy Settings (see page 155)

Selective Trigger-Based Purging

Each trigger in the user policy has its own Minimum Retention setting. This permits you to set a custom retention period for all events captured by a specific trigger. For example, you may want to retain events captured by an Application Monitor trigger for one month only, but retain events captured by an e-mail trigger for three years.

To set minimum retention periods for triggers

1. Expand the User Administration branch .
2. Choose the user or group whose policy you want to edit.
3. Click or right-click and choose Edit Policy.
4. In the User Policy Editor, browse to the trigger you want and display the trigger settings.
5. For any capture trigger, edit the Minimum Retention (Days) setting as required.

   For any control trigger, separate Minimum Retention (Days) settings are available for prohibited activity (that is, blockings and heeded warnings) and authorized activity (all other control events). Edit these settings as required.

   For all triggers, you can permanently exclude events from purges by selecting the Unlimited check box in the Policy Setting Properties dialog.
6. Save the policy. The new retention period becomes effective as soon as the new settings replicate to the target CA DataMinder machines.

Notes:

- Trigger-based minimum retention periods override the default retention period for the local machine (defined in the machine policy).
- Users with appropriate administrative privileges can override the expiry date of the retention period when reviewing events in the iConsole.

Turn off Purging

By default, database purging is turned off. If, after installation, you turned on database purging but subsequently need to turn it off you must edit the machine policy.

1. In the Administration Console, expand the Machine Administration branch.
2. Edit the policy for the machine or machines on which you want to turn off purging.

   For example, to turn off purging on all gateways, right-click the CMS and choose Edit Common Gateway Policy.
3. In the Machine Policy Editor, browse to the Data Management folder.
4. Set Purge Events on Replication? to False (clear the check box).
5. Set Database Purge Frequency (Days) to 0 (zero) days.
6. Save the policy.

   Database purging is turned off as soon as the new settings replicate to the target CA DataMinder machines.

More information:

Event Purging (see page 146)

Purge Policy Settings

To set up event purging for CA DataMinder machines, you must edit settings in the relevant machine policy.

Scheduled purges

To schedule regular purges, edit these settings in the Data Management folder of the local machine policy.

Minimum Retention Period (Days)

Confirm or reset this setting. It defaults to 1095 days, ensuring that the next purge removes all items more than three years old. Typically, but not always, this means events that have been retained in the local database for more than 1095 days and which have already been replicated.

Note: You can override this default minimum retention period in the user policy. Each capture and control trigger can specify a custom retention period for all events captured by that trigger.

Event Purge Frequency (Days)

By default, this is set to zero. Reset this to one day to schedule daily purges.

Event Purge Time (Minutes)

Specify at what time the purge runs. Particularly for gateways, you may want to run purges when there is little or no user activity to minimize the impact on machine performance. To specify the purge time, enter the number of minutes after midnight (local time). For example, enter 180 to specify a 3 a.m. purge. By default, this setting corresponds to 1 a.m.

Note: If you are editing the Common Client or the Common Gateway policies, you can enforce a setting for all client machines and gateways by clicking Enforce Items.

Purge performance

The following settings provide further control over purge operations:

Suspend Infrastructure During Purge?

You can choose whether to suspend the infrastructure during scheduled purges. Select this setting (set it to True) to automatically suspend the infrastructure while the scheduled purge runs (unless the infrastructure is already suspended).

Typically, you may want to suspend the infrastructure while performing other purge-related database activity or for performance reasons. For example, purging may be faster with foreign key constraints removed from certain tables. In this situation, we recommend that you pause replication activity while the purge runs to prevent new data being written to the database while these constraints are removed; suspending the infrastructure guarantees that all replication activity is paused for the duration of the purge.

Event Purge Batch Size

When purging a database, CA DataMinder can delete a batch of rows in a single operation. You can specify how many rows are included in each batch deletion. Larger batch sizes mean bigger database transactions and more DBMS locks. Note that a single purge operation typically includes multiple batch deletions.

Note: This setting applies only to the default purge process. It may not apply to custom purge processes.

Event Purge Temporary Storage Size

You can specify the maximum number of database rows that can be stored in a temporary table at one time.

For efficient purge processing, CA DataMinder retrieves events flagged for purging and stores them in a temporary database table. When the temporary table has been fully purged, CA DataMinder refills it with the next batch of events flagged for purging. This process repeats until the purge completes or times out. This setting prevents the temporary table becoming too large and adversely affecting performance.

Note: This setting applies only to the default purge process. It may not apply to custom purge processes.

Event Purge Timeout (Minutes)

In addition to specifying when a purge starts, you can also specify the maximum time (in minutes) that a database purge can run for. You may want to limit the purge duration so that, for example, it does not coincide with replication or import operations. When the timeout expires, the purge is terminated.

More information:

Event Purging (see page 146)
Minimum Retention Period (see page 150)

Diagnostics

More information:

Overview (see page 157)
Configure Diagnostics Collection (see page 158)
Replication Checkpoints (see page 160)
Configure Checkpoints (see page 162)
Diagnosing Missed Checkpoints (see page 163)

Overview

The CMS collects machine diagnostic data from all CA DataMinder servers and client machines in the machine hierarchy. This data underlies the diagnostic machine and user searches available in the Administration console. To minimize network impact, you can configure when and how this diagnostic data is collected.

Diagnostic Machine Searches

The Administration console includes a wide range of diagnostic machine searches. Typically, these are searches to identify machines that require your attention. For example, you can search for machines that are suspended or which cannot be contacted, or which are running out-of-date software.

In addition, CA DataMinder includes specific diagnostic support for replication problems in the form of checkpoints. These are replication markers sent to all CA DataMinder machines and which require an acknowledgment from each recipient. They enable administrators to check child machines are up-to-date in terms of policy updates and other infrastructure data. The Administration console includes several checkpoint-based machine searches.

Diagnostics Policy Settings

You can configure the CMS to control when it collects diagnostic data. You can also control the network impact by changing the number of collection threads and specifying how long it spends collecting this data. Finally, you can update the account login status for any anomalies identified in the diagnostic data.

To configure the collection of diagnostic data, you edit settings in the CMS or gateway machine policy. Browse to the Diagnostics policy folder.

More information:

Replication Checkpoints (see page 160)
Configure Diagnostics Collection (see page 158)

Configure Diagnostics Collection

To configure the collection of diagnostic data, you edit settings in the CMS or gateway machine policy. Browse to the Diagnostics policy folder and edit these settings:

Collection Time

Defaults to 720, equivalent to 12.00 pm (noon). This setting specifies when, or how often, diagnostic data is collected. This is dependent on the Collection Frequency setting.

If the Collection Frequency (see below) is:

- Set to zero, the Collection Time setting specifies the number of minutes between each collection run. If the Collection Time and Collection Frequency are both zero, automatic scheduled collections are disabled.
- Set to one or more days, the Collection Time setting specifies the number of minutes past midnight when data collection begins.

Collection Frequency

Defaults to 1. This setting indicates how often (in days) diagnostic data is collected.

If the Collection Frequency is zero, data is collected more frequently than one a day; this depends on the Collection Time setting—see above.

If the Collection Frequency and Collection Time are both zero, automatic scheduled collections are disabled

Collection Period

Defaults to zero. This setting determines how long (in minutes) the CMS or gateway spends collecting diagnostic data.

For example, if the Collection Frequency is 1 and the Collection Period is 120, then diagnostics are collected daily over a two-hour period.

If the Collection Period is zero, the server automatically calculates an appropriate collection period.

Number of Collection Threads

This setting is only invoked if there has been no communication between the parent and child machine. It specifies the maximum number of additional threads used simultaneously to collect and process diagnostic data from child machines. It defaults to 10.

To minimize network impact, diagnostic data is collected as part of the normal communications between a parent and its child machines. But if there has been no communication between these machines during the collection period, additional threads are created specifically to actively collect this diagnostic data.

You can increase concurrency by raising the number of collection threads. This reduces the time needed to collect the data but also has a greater impact on your network. Alternatively, you may choose to reduce the number of collection threads so that data trickles back to the parent server, lengthening the collection time but reducing network load.

Session Record Expiry Period

Defaults to seven days. This setting is used to rectify inaccurate session records identified when processing the diagnostic data. That is, a user account is logged out of CA DataMinder but the session record on the parent server indicates the user is still logged in. For example, this may happen if problems occur when uninstalling a client machine.

How does this setting work? If diagnostic data from a child machine indicates the machine has not been running for longer than this expiry period, all open machine and user sessions for this machine are updated to the Logged Out state.

If the Session Record Expiry Period is zero, session records are never cleared by this method.

More information:

Diagnostics (see page 156)

Replication Checkpoints

Checkpoints enable administrators to check child machines are up-to-date in terms of policy updates and other infrastructure data (that is, user and machine details).

The CMS generates a checkpoint record and adds this to the replication queue, from where it is subsequently sent to all child machines. Each child machine then returns a checkpoint acknowledgment. This is a confirmation that the child machine has received all infrastructure updates sent prior to this latest checkpoint. Note that acknowledgments are fast-tracked back to the CMS to allow rapid diagnosis of your CA DataMinder deployment.

Checkpoints can be generated automatically, for example, at 01.00 am every day or after every 1,000 infrastructure updates. You can also manually generate checkpoints and configure how long checkpoints and their acknowledgment are retained in the CMS database.

How long are checkpoints retained?

By default, checkpoints and acknowledgments are retained in the CMS database for 60 days, but you can configure this in the CMS machine policy.

Automatic checkpoints

You can configure the CMS to generate checkpoints automatically, at regular intervals or after a specified number of infrastructure updates. To do this, or to disable automatic checkpoints, you edit the CMS machine policy.

Automatic checkpoints are assigned a checkpoint ID and description, both of which can be used when running a custom administration search for machines.

Automatic checkpoints are assigned one of two checkpoint descriptions:

- Scheduled: Specifies a regular checkpoint generated using the Checkpoint Time and Checkpoint Frequency machine policy settings.
- Triggered by update count threshold: Specifies a checkpoint generated by the Update Count Threshold machine policy setting.

Manual checkpoints

If required, you can manually set checkpoints. For example, you may want to send a custom checkpoint after making changes to your user hierarchy or after running a major Account Import job. To set a manual checkpoint:

1. Choose Tools, Generate Checkpoint.
2. In the resulting dialog, specify a description of the checkpoint and click Generate.

A checkpoint ID appears in the dialog. The checkpoint ID can be copied to the Windows clipboard for use when running a custom administration search for machine.

3. Close the dialog.

Note: The description, along with the checkpoint ID, is stored in the Wgn3Checkpoint database table.

More information:

Diagnostics (see page 156)
Run a New Administration Search (see page 46)

Configure Checkpoints

To configure automatic checkpoints and to specify the checkpoint retention period, you edit settings in the CMS machine policy. Browse to the Checkpoints policy folder:

Checkpoint Time

Defaults to 1140 (19 hours or 7.00 pm). This setting specifies when checkpoints are generated, or how often they are generated.

This setting is dependent on the Checkpoint Frequency setting (see below). If the Checkpoint Frequency setting is:

Set to zero, the Checkpoint Time setting specifies the number of minutes between each generated checkpoint. If the Checkpoint Time setting is also set to zero, scheduled checkpoints are disabled.

Set to one or more days, the Checkpoint Time setting specifies the number of minutes past midnight when each checkpoint is generated.

Note: If a new checkpoint is scheduled but there have been no infrastructure changes since the last checkpoint, a new checkpoint is not generated.

Checkpoint Frequency

Defaults to 1. This setting indicates how often (in days) checkpoints are generated.

If the Checkpoint Frequency is zero, then scheduled checkpoints are either disabled or generated more frequently than one a day; this depends on the Checkpoint Time setting.

Update Count Threshold

Defaults to zero. This setting specifies the number of infrastructure updates that trigger a new checkpoint. If this setting is zero, the update count threshold is disabled and checkpoints are not generated.

What is a suitable value for this setting? Unfortunately, we cannot give precise guidelines. A simple policy update, perhaps affecting a dozen trigger settings, may only comprise two infrastructure updates (to the policy and blob database tables). Conversely, a major restructuring of a typical user hierarchy, with its attendant impact on policy tables, the group hierarchy, e-mail address tables and so on, can easily comprise tens of thousands of infrastructure updates. We recommend that you leave this threshold set to zero and only change this under the guidance of CA technical staff.

Checkpoint Retention (days)

Defaults to 60. This setting specifies how many days checkpoints and their acknowledgments are retained on the CMS. Set this value to zero to permanently retain checkpoints and acknowledgments.

Disabling automatic checkpoints

To fully disable automatic checkpoints, set the following three policy settings to zero: Checkpoint Time, Checkpoint Frequency and Update Count Threshold.

More information:

Diagnostics (see page 156)

Diagnosing Missed Checkpoints

The Administration console provides a number of predefined searches based on missed checkpoints. For example, you can search for machines that have failed to acknowledge the latest checkpoint, or machines which have not acknowledged a checkpoint for three days.

After identifying these machines, we suggest that you analyze the CA DataMinder log files on these machines and their parent servers to determine the cause of the missed checkpoints. Under normal conditions, after the problem has been fixed any outstanding infrastructure updates, including missed checkpoints, are then automatically replicated to those child machines when they signal to their parent server that they are ready to start receiving updates again.

You can run an Administration search to identify machines that have failed to acknowledge recent checkpoints.

More information:

Diagnostics (see page 156)
Run an Existing Administration Search (see page 45)

Chapter 10: Machine Policy Settings

A machine policy contains settings that govern how CA DataMinder computers manage their database of captured events.

More information:

Edit a Policy (see page 164)
Edit Common Machine Policies (see page 164)
Policy Navigation (see page 165)
What Is in a Machine Policy? (see page 165)

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.

More information:

Policy Navigation (see page 165)

Edit Common Machine Policies

By default, new endpoint computers machines inherit the Common Client Policy and new gateways inherit the Common Gateway Policy.

To edit the common machine policies

1. Log on to the Administration console using an account that has the 'Policies: Edit policy' administrative privilege.
2. Expand the Machine Administration branch.
3. Right-click the CMS and click Edit Common Client Policy or Edit Common Gateway Policy.

More information:

Edit a Policy (see page 164)

Policy Navigation

In the Policy Editor, you can quickly navigate around a policy using hyperlinks and the Back and Forward buttons.

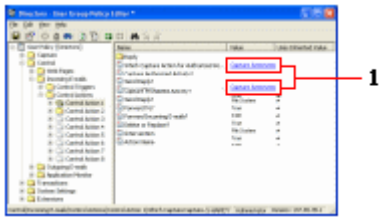
Back and Forward buttons

Use these to jump back to previously selected policy items.

- Click Back to go back to the policy setting or folder that you previously selected.
- Click Forward to return to the policy item you selected before you clicked Back.

Hyperlinks

Some settings are hyperlinked to a dependent setting or folder. For example, each control action has two settings that specify capture actions. Click the hyperlink to jump to the specified capture action.



1 Policy Editor example hyperlinks

Note: These hyperlinked settings are available only in the user policy; there are no equivalent hyperlinks in the machine policy.

Keyboard shortcuts

You can use the arrow keys to navigate through the policy settings. To open a hyperlink, press Ctrl+L.

Note: This keyboard shortcut works only when the setting containing the hyperlink is selected in the right-hand pane.

What Is in a Machine Policy?

More information:

Infrastructure Settings (see page 166)
Policy Engine Settings (see page 178)
Client File System Agent Settings (see page 180)
Client Network Agent (see page 187)
Central Management Server Settings (see page 188)

Infrastructure Settings

The CA DataMinder infrastructure is a collection of software components that enable CA DataMinder computers to operate, communicate with each other, and protect confidential data.

More information:

Security Settings (see page 166)
Data management Settings (see page 167)
Replication Settings (see page 168)
Logging Settings (see page 169)
Filter Setting (see page 175)
Account Import Settings (see page 175)
Lookup Cache Management Settings (see page 176)
Diagnostics Settings (see page 177)

Security Settings

These settings control when CA DataMinder uses encryption. They apply to records in the local database and data transfers across the network.

Encrypt Stored Data

If required, you can encrypt records in the local database.

On client machines, this applies only to policy data. You cannot encrypt captured data such as e-mails or Web pages.

On the CMS, all database records are encrypted. These include user and machine account and policy details for each user and machine, plus all captured events.

Encryption Key Thresholds (Volume and Interval)

You can specify the thresholds (the volume of encrypted data or an elapsed time period) that trigger an automatic change to the encryption key.

Communications Encryption

You can specify varying levels of encryption when CA DataMinder machines send data across the network.

Cache CMS Credentials

If these are set to cache, you can skip the console logon dialog providing you have already successfully logged on to the CMS during the current session.

Data management Settings

These settings cover database management on CA DataMinder machines. They determine whether data compression is used, how often the local databases is purged, and how CA DataMinder handles free disk space.

EMC Centera Integration

These settings cover the optional parameters to configure the integration of your Centera device. For example, they determine the number and size of BLOB files stored in a Centera device, and the method used to calculate the Content Address from BLOB files.

IBM DB2 Content Manager Integration

These settings cover the optional parameters to configure the integration of your IBM DB2 Content Manager. For example, they determine the number and size of BLOB files stored in the Content Manager, and the credentials for the Content manager Interface Service.

Compression

If required, you can compress stored data on CA DataMinder servers and client machines. Specifically, you can compress the 'blobs' (Binary Large Object files), containing policy data and, on the CMS and gateways, captured data.

Event purging

For each machine, you determine the frequency and time of each purge, plus the minimum retention period that captured events are retained before they are earmarked for purging. Other settings provide further control over purge operations. For example, you can choose to suspend the CA DataMinder infrastructure during purge operations or you can specify a purging timeout.

Free disk space

For each machine, you can specify a warning level and an error level of free disk space. You can also specify how often free disk space is checked. When free disk space falls below the warning level, CA DataMinder adds a series of warnings to the Activity logfile. When free disk space falls below the error level, the CA DataMinder infrastructure is suspended.

Remote Data Management

These settings cover the optional parameters to configure the integration of the temporary object store. For example, you can configure how long events remain in the object store before being deleted. For details, see the *Platform Deployment Guide*.

More information:

Purge Policy Settings (see page 155)
Monitoring Free Disk Space Overview (see page 138)

Replication Settings

These settings determine how often CA DataMinder machines send notification of newly captured data or local infrastructure changes. These notification messages act as triggers for data replication between CA DataMinder machines. These settings also cover connection management on CMSs and gateways.

Connection management

Available for CMSs and gateways only. These settings cover connection management on a CMS or gateway server. They determine the maximum number of simultaneous connections to client machines, and the maximum number of days that infrastructure changes intended for offline client machines are retained in the CMS cache (the 'cache timeout') before being purged.

Note: Any offline client machines that fail to reconnect to the CMS and retrieve the latest infrastructure changes before the cache timeout expires are flagged as 'out-of-sync'. When an out-of-sync machine next reconnects to the CMS or gateway, it automatically resynchronizes all of its infrastructure data.

Notification of captured data

You determine how often a client machine notifies the CMS about newly captured data. When the CMS receives this notification, it transfers the captured data from the client to the CMS and the client stops sending notifications.

Notification of infrastructure changes

You determine how often client machines and the CMS notify each other of new infrastructure changes such as policy edits or user account updates. When the recipient machine receives this notification, it determines if it needs the update; if so, it requests the details. As soon as the recipient machine has processed the notification, the sender machine stops sending notifications.

Logging of replication failures

You can specify how soon CA DataMinder begins logging failures by a source machine to contact its target machine.

Replication over slow links

You can disable the replication of captured data when the connection to the CMS or Gateway is over a Wide Area Network or dial-up (modem) connection.

Compression

If required, you can compress policy data and captured data before transmitting it across the network between CA DataMinder machines.

Batch size of captured data

When a child machine replicates captured data to its parent server, it sends events in batches in order to conserve network bandwidth. This setting specifies the maximum number of KBytes in each batch.

Note: It is very unlikely that you will ever need to change the default batch size.

Batch size of infrastructure data

When a parent server replicates infrastructure changes (for example, local policy changes) to a child machine, it sends data objects in batches in order to conserve network bandwidth. This setting specifies the maximum number of KBytes in each batch.

Note: It is very unlikely that you will ever need to change the default batch size.

Replication holding cache

You can set up scheduled operations to automatically move events out of the replication holding cache at regular intervals. For full details, see the *Platform Deployment Guide*; search for 'reset the replication holding cache'.

Logging Settings

CA DataMinder maintains logs for all product components to record significant activity or events. For log files controlled or generated by the CA DataMinder infrastructure, machine policy settings control which infrastructure operations are logged.

General Log Configuration

You can edit these settings in the Infrastructure > Logging policy folder:

Maximum Number of Log Files

Specifies the maximum number of log files. This limit applies separately to each type of log (that is, for each type of logfile you can generate files up to the maximum number). When this maximum number is exceeded, the oldest log file is deleted.

Maximum Size of Log Files

Specifies the maximum size (in KB) for each log file. When the current log file reaches its maximum size, CA DataMinder creates a new log file.

Note that this size limit does not apply to Account Import log files.

Write to Windows Event Log

Specifies the default handling for copying CA DataMinder log entries to the Windows Application log.

Write to Syslog Server

Specifies the default handling for copying CA DataMinder log entries to a Syslog server such as ArcSight.

Activity Log Configuration

In the Infrastructure > Logging > Activity subfolder, you can optionally record the following activities:

Machine and User Logins

You can record login and logout times and, for user logins, you can also record failed account creation attempts.

Machine and User Administration Changes

These changes include accounts being created, modified or deleted. You can also record this information in the User Administration log file.

Policy Changes

These include any saved changes to user or machine policies.

Cache Actions

These include cache changing and purge activity involving the temporary object store, and plus cache preload and clear down operations associated with the internal user cache and e-mail address cache (used to optimize event processing).

Storage Connector Events

These refer to events associated with third party object stores. CA DataMinder uses storage connectors to integrate with third party object storage solutions. The range of logged events includes object store connections and disconnections, storage queue activity and data retrieval.

Policy Incident Log Configuration

(Only available in the CMS machine policy.)

These logs are created on the CMS only. In the Infrastructure > Logging > Policy Incidents subfolder, you can optionally record the outcome each time a user policy trigger fires. The log includes both event-level and trigger-level entries. Edit these settings:

Log Policy Incidents Locally To File

If enabled, CA DataMinder writes entries to the policy incident log on the CMS.

iConsole Address

Set this to the fully qualified domain name or IP address of a machine hosting the iConsole application server. For example:

CMS-HARDY.unipraxis.com

This address is incorporated into the event URL in each log entry (see below). Administrators can browse to this URL to view the associated incident in an iConsole.

Format of Event URL

You do not normally need to edit this policy setting. It specifies the format of the event URL included in the log message. Users can browse to this URL to view the event in the iConsole.

Replication Log Configuration

In the Infrastructure > Logging > Replication subfolder, you can optionally record when a CA DataMinder machine receives replicated data. In all cases, you can choose to record summary information (when replication starts and completes, and how many objects were successfully replicated) or you can record detailed information (log entries for each successfully replicated object). Edit these settings:

Captured Data

This can include captured or imported e-mails, Web pages, IM events, file events, and so on, plus any associated trigger details, event attributes, and policy actions.

Infrastructure Data

This includes changes to user and machine accounts or policy updates.

Critical Data

This typically includes data recorded for diagnostic purposes. For example, when a machine becomes suspended a notification is replicated to the CMS.

System Log Configuration

In the Infrastructure, Logging, System subfolder, you can optionally record any infrastructure errors while the CA DataMinder service is running. Under normal conditions, this log is empty.

Note: Any errors detected when the CA DataMinder service starts up are written to the file wgninfra.out. Find this file in the same folder as the System log.

User Administration Log Configuration

In the Infrastructure, Logging, User Administration subfolder, you can optionally record changes made to user accounts or groups. You can also record these changes in the Activity log; see above.

External Logging

Settings in the Infrastructure, Logging, External Logging subfolder enable CA DataMinder to copy log entries to the local Windows Application log and to Syslog servers.

More information:

Overview (see page 111)
External Logging Settings (see page 173)

External Logging Settings

Settings in the Infrastructure > Logging > External Logging subfolder enable CA DataMinder to copy log entries to the local Windows Application log and to Syslog servers.

Windows Event Log

This subfolder contains Log Detail settings for each infrastructure-maintained log file:

<Type> Log Detail

Each of these settings specifies which messages are copied to the Windows log and overrides the default log level. In each case, you can choose 'None', 'Errors Only', or 'Errors and Warnings'. You can also choose:

'Use Default' to use the default log level defined by the Write to Windows Event Log setting.

'All Messages'. Any message written to the CA DataMinder log is also copied to the Windows log.

Syslog n

There are three Syslog subfolders, allowing you to specify up to three different Syslog servers. Each subfolder contains:

<Type> Log Detail

Each of these settings specifies which messages are copied to the Syslog server and overrides the default log level. In each case, you can choose 'None', 'Errors Only', or 'Errors and Warnings'. You can also choose:

- 'Use Default' to use the default log level defined by the Write to Syslog Server setting.
- 'All Messages'. Any message written to the CA DataMinder log is also copied to the Syslog server.

Server Name

Specifies the IP address or fully qualified domain name of the Syslog server.

Server Port

Specifies the port number that the Syslog listens on. By default, Syslog servers use port 514.

Maximum Message Length

Specifies the maximum length (in characters) for log messages copied to a Syslog server.

Client Port

Specifies the port(s) that CA DataMinder uses to send log messages to Syslog server. If required, you can specify a range of consecutive port numbers (such as 510—515) or a comma-separated list of port numbers and ranges (such as 501,505,510—515).

Syslog Protocol

Specifies the format for data transfers to the Syslog server. Choose either:

- 'IETF RFC 3164'. All Syslog servers support this protocol.
- 'IETF Syslog Internet Draft Document'. This is specifies an extension to the RFC 3164 protocol.

We recommend that you choose the RFC 3164 protocol unless you are certain that your Syslog server supports the extension published in the Internet Draft Document.

Message Format:

Choose either:

- 'Common Event Format'. Choose this option if your Syslog server supports CEF. For example, ArcSight uses CEF. If you do choose CEF, some further policy configuration is needed.
- 'Unformatted Data'. If your Syslog server does not support CEF, choose this option.

Common Event Format Configuration

Each Syslog n policy folder (see above) contains a Common Event Format Configuration subfolder. If you specify 'Common Event Format' as the Message Format (see above), settings in this subfolder let you change the severity values assigned by CA DataMinder to CEF messages.

Error Messages Severity Value

Defaults to 8. This severity value is assigned to error messages and high severity events when sent to Syslog servers as CEF messages.

Warning Messages Severity Value

Defaults to 5. This severity value is assigned to warning messages and medium severity events when sent to Syslog servers as CEF messages.

Information Messages Severity Value

Defaults to 1. This severity value is assigned to Information messages and low severity events when sent to Syslog servers as CEF messages.

Note: CEF messages must include an event severity value between 0 and 10.

More information:

Logging Settings (see page 169)

Filter Setting

This setting is for Event Import operations.

User filter

This filter enables you to modify Event Import operations to exclude or only include users with specific account attributes. For example, if your user accounts include a 'Country' attribute, you configure import jobs to only import e-mails owned by users in a specific country.

Note: For full details about filtering Event Import operations, please refer to the *Archive Integration Guide*; search for 'filtering event import operations'.

Account Import Settings

These machine policy settings are for Account Import operations.

Maximum Number of Threads

This setting specifies the maximum number of concurrent 'worker' threads used by Account Import.

Auto-commit threshold

This setting specifies the total number of database operations that can be performed by all transactions before they are all committed to the database.

Note: When a transaction is successfully completed, it releases any DBMS locks.

Retry count for aborted transactions

This setting specifies the maximum number of times Account Import will try to roll back and retry an aborted transaction. If this limit is reached, Account Import fails and an error message is written to the log file.

Note: An error message is also written to the Account Import log file at the time the transaction aborts.

Lookup Cache Management Settings

These settings are used to configure Data Lookup caches.

Disable Caches

You can specify that details retrieved from the CMS database for Data Lookup operations are not cached.

Disable Preload

CA DataMinder can preload the Data Lookup cache with information from the CMS database before running any lookup operations. This can speed up subsequent Data Lookup operations, as the information is already stored locally. You disable this preload.

Maximum Entries

Specify the maximum number of entries in the Data Lookup caches.

Maximum JVM Memory (Percent)

Specify the maximum percentage of JVM memory that each individual cache will use.

Diagnostics Settings

These settings determine how CA DataMinder servers collect diagnostic data from child machines and how often replication checkpoints are sent to child machines. They allow you to configure operations to minimize network impact.

Checkpoints

These settings determine when and how often CA DataMinder generates replication checkpoints. These are sent to all child machines.Each child machine then returns a checkpoint acknowledgment. This is a confirmation that the child machine has received all infrastructure updates sent prior to this latest checkpoint.

Checkpoint Time and Checkpoint Frequency

You can specify when checkpoints are generated or how often they are generated.

Update Count Threshold

You can specify the number of infrastructure updates that trigger a new checkpoint.

Checkpoint Retention

You can specify how many days checkpoints and their acknowledgments are retained on the CMS.

Collection Time and Collection Frequency

You can specify when, or how often, diagnostic data is collected.

Collection Period

This setting specifies how long the CMS or gateway spends collecting diagnostic data. This enables you to limit the network impact.

Number of Collection Threads

To minimize network impact, diagnostic data is collected as part of the normal communications between a parent and its child machines. But if there has been no communication between these machines during the collection period, this setting creates additional threads to actively collect this diagnostic data.

Session Record Expiry Period

This setting is used to rectify inaccurate session records identified when processing the diagnostic data. If diagnostic data indicates a machine has not been running for longer than this expiry period, all open machine and user sessions for this machine are updated to the Logged Out state.

Policy Engine Settings

These settings configure the local policy engine. Before running a policy engine, you need to specify, for example, how many policies it can hold at one time and how many events it can process simultaneously:

Settings to Determine Which User Policy Gets Applied

These settings determine how the policy engine handles events when it does not recognize the associated user or when user information is unavailable.

Important! For all of these settings, you must restart the policy engine any changes to take effect!

Unknown Internal Sender

Policy engines use this setting to apply policy to e-mails sent from unrecognized users within your organization. For example, this can happen if a new recruit has an account in Active Directory but no CA DataMinder account has been created for them yet.

The setting specifies the name of a CA DataMinder user. It defaults to UnknownInternalSender; this account is created automatically when you install a CMS. The policy engine applies this user's policy if the sender's address is internal (that is, it matches an Internal E-mail Address Pattern—see below) but no corresponding CA DataMinder user account exists.

External Sender

Policy engines use this setting to apply policy to external e-mails. That is, e-mails sent from someone outside your organization.

The setting specifies the name of a CA DataMinder user. It defaults to ExternalSender. This account is created automatically when you install a CMS. The policy engine applies this user's policy if the sender's address is external (that is, it does not match an Internal E-mail Address Pattern—see below).

Internal E-mail Address Pattern

Policy engines use this setting to detect e-mails sent by users within your organization.

This setting specifies a list of internal e-mail address patterns. Policy is only applied to the e-mail if the sender's e-mail address matches an internal address pattern. Similarly, Address Book (MAPI) lookup operations are only performed for recipients with internal addresses.

Default Policy for Files

This setting specifies the name of a CA DataMinder user. It defaults to DefaultFileUser. This user account is created automatically when you install a CMS.

Policy engines use this setting to apply policy to files if no other means are available to determine the policy participant. For example, if an FSA scanning job specifies a ser account that does not exist, the policy engine applies the Default Policy for Files to the scanned file.

Default Policy for Classification

The setting specifies the name of a CA DataMinder user. It defaults to DefaultClassificationUser. This account is created automatically when you install the CA DataMinder Content Classification Service (CCS).

Policy engines use this setting to classify documents forwarded to the CCS from external applications such as CA SiteMinder.

Other Settings

Maximum Number of Loaded Policies

You can optionally define the maximum number of user policies that the policy engine can hold in its memory at one time. Because each policy requires a significant amount of memory, this setting can prevent excessive memory usage.

Maximum Number of Concurrent Operations

You can optionally define the maximum number of e-mails that can be processed simultaneously by a policy engine. This can prevent a performance slowdown on heavily loaded policy engines.

Perform LDAP directory lookups?

This setting is provided for diagnostic purposes only. It specifies whether the policy engine can retrieve e-mail address details and distribution list members from an LDAP directory.

Important! We strongly recommend that you do not change this setting!

Retention Period for Unused Policies

This setting defines the frequency of policy timeouts. That is, the amount of time a policy engine retains a policy that has not been used. After this period of time, the policy is unloaded.

Deadlock Detection Timeout (Seconds)

This setting is designed to maintain processing capacity. It specifies how long a thread must be inactive before the policy engine considers the thread to have stalled and creates a new processing thread.

Embedded Message Identification

This setting enables policy engines to detect 'embedded content' e-mails (that is, EML e-mails contained embedded IM conversations, Bloomberg messages or other communications such as eFaxes). It enables policy engines to set the event type as 'embedded IM', 'Bloomberg' or 'eFax' and, for IM conversations, to extract or set the IM network.

Retention Period for Unused Policies

This setting defines the frequency of policy timeouts. That is, the amount of time a policy engine retains a policy that has not been used. After this period of time, the policy is unloaded.

Deadlock Detection Timeout

This setting is designed to maintain processing capacity. It specifies how long a thread must be inactive before the policy engine considers the thread to have stalled and creates a new processing thread.

Client File System Agent Settings

These settings configure Client File System Agent (CFSA) behavior on client machines. They determine how the CFSA handles:

- *Data in use*. This refers to files being copied to removable devices, to CDs and DVDs, or to network locations. These policy settings determine whether a user is allowed to copy files to these destinations.
- *Data at rest*. This refers to files saved on the local hard disk. These policy settings determine how often the CFSA scans the local hard disk.

More information:

Data In Use Protection Folder (see page 180)
Data At Rest Protection Folder (see page 186)

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 181)
Network Locations Folder (see page 183)
File Sync Providers Folder (see page 185)

Removable Devices Folder

Edit settings in this folder to protect files 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.

lsass.exe always included

By default, lsass.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 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.

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.

More information:

File System Scan Configuration Folder (see page 187)

File System Scan Configuration Folder

These settings determine when and how often the CFSA scans the local hard disk. They specify the time and day when the full scan begins, plus the number of days between each scan.

Start Time

This is specified as ‘minutes after midnight’, so enter 60 to specify a 1am start time.

Start Day

This can be any day of the week or ‘Next’. This specifies when the scan first runs; when it next runs depends on the Frequency. If you choose Next, the scan starts at the next occurrence of the Start Time; this could be later today or tomorrow.

Frequency (days)

This specifies how often the scan runs. For example, to run a scan every Sunday, set the Start Date to Sunday and the Frequency to 7.

To set up daily file scans

1. Set the Start Time as required.
2. Set the Start Day to ‘Next’ and the Frequency to 1.

   Note: Do **not** set the Start Day to a specific day of the week; if the client machine is restarted, the next scan will not run until the next occurrence of the Start Day.

Client Network Agent

These settings configure Client Network Agent (or 'network agent') behavior on endpoint computers. They determine how the network agent handles network activity in specific applications or browsers.

You can edit these settings to exempt specific applications or browsers from policy control. For example, you can exempt Microsoft Word when it is used to check in or check out documents from a SharePoint site.

Note: By default, the network agent is configured to monitor web activity for most common browsers and Microsoft Office applications, including Microsoft Internet Explorer, Mozilla Firefox, Opera, and Google Chrome.

Central Management Server Settings

These settings apply exclusively to operations on the CMS. They cover account handling for unknown users or machines, database management and CMS single sign-on.

New user accounts

These settings determine how the CMS handles logon attempts by new users who have no account on the CMS.

Note: Note the domain prefix requirement for administrator-created new accounts.

New machine accounts

These settings determine how the CMS handles the CA DataMinder infrastructure starting on machines that are not registered with the CMS.

Default group for new users

You can specify whether client machines are permitted to specify a default parent group for new CA DataMinder users created automatically on the client.

Single sign-on

This setting determines whether users skip the logon dialog when they start up a CA DataMinder console.

Undelete user accounts

This setting determines whether a previously deleted user account can be recreated if a new user is created with a matching user name.

Move groups

This setting defaults to False and determines whether user groups can be moved within the group hierarchy.

Important! Changing this setting to True can potentially cause row level security issues!

Prohibit password characters

This setting determines which characters are not allowed as part of a user-created password within the Administration console, Data Management console, or iConsole.

More information:

Windows Authentication and New Users (see page 197)
Enable Single Sign-on (see page 60)
Recreate Users (see page 198)
Move Users Between Groups (see page 202)

Chapter 11: Mapping E-mail Addresses to Users

This section contains the following topics:

Overview (see page 189)
Which Features use Address Mapping? (see page 190)

Overview

Certain CA DataMinder features need to identify the owners of captured or imported e-mails based on the addresses of the sender or recipients. These features are: policy engines; User Attribute (userattr) lookup commands in e-mail control triggers; and the Event Import utility.

To minimize storage and optimize performance, CA DataMinder stores events and users separately in the CMS database. Unlike in previous versions, it does not assign e-mails or IM conversations directly to CA DataMinder users. Instead, it identifies 'event participants' and maps these participants onto CA DataMinder users based on e-mail addresses. For full details, see the *Platform Deployment Guide*; search the index forsearch for 'e-mail address mapping'.

More information:

Which Features use Address Mapping? (see page 190)

Which Features use Address Mapping?

Which features use e-mail address mapping?

CA DataMinder needs to map e-mail addresses onto individual users for 'multiple participant' events. Specifically, address mapping is used by the following CA DataMinder features to associate imported e-mails and IM conversations, and e-mails captured on an Exchange server, with specific CA DataMinder users:

Policy engines

Before a policy engine can apply policy triggers to an intercepted e-mail, it needs to map the sender's e-mail address to a CA DataMinder user. The mapping identifies the e-mail owner and determines which policy to apply.

If the policy engine is unable to map an e-mail address to an existing CA DataMinder user, the DefaultUser and FallbackUser registry values on the policy engine hub determine which policy is applied.

User attribute data lookup

Before CA DataMinder can evaluate control triggers based on user attribute (userattr) lookup commands, it must map the recipients of an outgoing e-mail (or the sender of an incoming e-mail) onto CA DataMinder users. It can then evaluate the lookup command, comparing the attributes of the recipients (or the sender of an incoming e-mail) against the test criteria.

If the lookup command is unable to map a recipient onto an existing CA DataMinder user, the command typically evaluates to False so the trigger does not activate.

Event Import

Unlike in previous versions of CA DataMinder, Event Import does not assign e-mails or IM conversations directly to owners. Instead, it identifies 'event participants' and associates an e-mail address with each participant. Under normal conditions, address mapping is not required while an import job is running. Instead, it is used subsequently to associate imported events with specific CA DataMinder users during event searches.

However, address mapping is used during an import job if a 'user attribute' filter is specified. This enables import jobs to exclude or only include all e-mail or IM conversations associated with CA DataMinder users who have specific account attributes.

Import Policy

Import Policy provides a mechanism for applying policy triggers to imported e-mails directly before they are stored in the CMS. For import policy jobs, address mapping is not used during the import phase. Instead, address mapping is used by the policy engines to determine which policy to apply.

More information:

Overview (see page 189)

Chapter 12: User Administration

The User Administration screen is where you manage user accounts and user groups. You can organize users into hierarchical groups, assign administrative privileges, and set passwords for individual users. You can also launch the User Policy Editor directly from this screen.

This section contains the following topics:

Administrators (see page 193)
User Accounts (see page 195)
User Groups (see page 199)
Export the user Hierarchy (see page 203)
User Properties (see page 204)
Exempt Users (see page 228)
Account Import (see page 230)

Administrators

CA DataMinder creates a Primary Administrator account when you install the CMS. You can use this account to create additional administrators in the Administration console.

All CA DataMinder administrators have the 'Administrator' user role. This role confers the full set of administrative privileges. All CA DataMinder administrators, including the Primary Administrator, have equal administrative authority.

Furthermore, you cannot change the administrative privileges assigned to the Administrator role and you cannot withdraw privileges from an individual administrator.

Also, all administrators use the Unrestricted security model and have no management group. Consequently, their administrative authority extends to all users. It is *not* restricted to specific user groups.

Note: If the Unrestricted security model is not enabled on your CMS, enable it (see page 33) before you create additional administrators.

More information:

Administrator Responsibilities (see page 194)
Default User Roles (see page 221)

Administrator Responsibilities

Administrators have the following responsibilities:

User Administration

Administrators must organize new users into a hierarchy and maintain the hierarchy. You also need a strategy for creating other administrators.

Organizing new users into a hierarchy

Before rolling out CA DataMinder across your organization, determine how you handle new users. Do you want to import user details into CA DataMinder from an existing source such as Active Directory? Can new users enroll themselves? You also need to organize users into groups. You can do this manually, or you can synchronize your CA DataMinder hierarchy of users and groups with an external source.

These issues are fully described in the 'Before You Start Using CA DataMinder' chapter of the *Platform Deployment Guide.*

Maintaining the user hierarchy

Your hierarchy of users and groups will require routine maintenance. For example, you may want to reorganize user groups to cater for users with particular policy requirements. This allows fast and selective rollout of policy changes. For example, you may decide to group together all users who are in constant email contact with customers.

Creating administrators

To share the administrative workload, you can promote ordinary users into administrators or managers by reassigning them to the appropriate user role. You can limit the scope of their administrative authority by specifying their management groups.

Machine Administration

Machine administration involves the following tasks.

Post-CMS installation

After you install the CMS but before you roll out CA DataMinder across your organization, you must configure your CMS policy, and the common client and gateway policies (these common policies are applied automatically to new machines). Key policy areas that you must consider include database purging and the management of free disk space.

These issues are fully described in the 'Before You Start Using CA DataMinder' chapter of the *Platform Deployment Guide.*

Routine maintenance

You must verify that all CA DataMinder computers are running the current versions of the software and that their individual machine policies are appropriate for your network environment. For example, you will need to ensure that replication, database purging and free disk space settings have sensible values. To optimize data flows across your network, you may also need to occasionally reorganize the allocation of client machines to each gateway.

Data security

You also need to consider data security. This covers encryption, database backups, and database purging.

Encryption

All events captured by CA DataMinder (emails, files, web pages and so on) is replicated across your network and stored on the CMS. These data transfers and the stored data itself must be secure. Configure the machine policies to encrypt this event data.

Backups

We recommend that you make a full backup of your CA DataMinder database on the CMS at least once per week, and incremental backups on a daily basis.

Database purging

We strongly recommend that you turn on database purging in the common gateway policy and common client policy. Regular purges prevent free disk space falling to dangerously low levels on your CA DataMinder computers, which in turn would cause the CA DataMinder infrastructure to be suspended.

Note: On a suspended endpoint computer, policy controls continue to operate (for example, emails are blocked) but the resulting events are not saved. For example, you cannot search for emails that were blocked while an endpoint was suspended.

Note: Administrators do not normally manage user policies. Users with responsibility for managing user policies are assigned to the 'Policy Administrator' user role.

User Accounts

More information:

New user Accounts (see page 196)
Delete Users and Groups (see page 198)
Recreate Users (see page 198)

New user Accounts

More information:

Add New Users (see page 196)
Windows Authentication and New Users (see page 197)

Add New Users

There are three ways to add new users.

Import users from an external source

You can import user details from an external data source. This is the method typically used by customers. To do this, use the Account Import wizard.

Add new users automatically

After you have installed the CA DataMinder Client Integration software on a user's computer, the user can add themselves to the user list.

1. Configure the CMS machine policy to automatically create accounts for unrecognized users.

   Specifically, configure the 'Account Handling for New Users' setting.

2. CA DataMinder creates a new user account automatically when an endpoint agent needs to apply policy to user activity. For example, if the Outlook endpoint agent is installed on a user's computer, CA DataMinder creates a new user account when the user next starts Outlook.

   CA DataMinder adds the new user account to the Default user group. It generates a user name for the new account based on Microsoft Windows authentication.

   Important! CA DataMinder cannot automatically create accounts for users whose names contain Far Eastern characters.

Add new users manually

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 a group for the new user.
3. Right-click the group and click New User.
4. Enter a name and specify the properties in the New User dialog.

More information:

New user Accounts (see page 196)

Windows Authentication and New Users

Microsoft Windows user authentication is used to automatically generate new user accounts. When the user next starts up their browser or e-mail application after the CA DataMinder Client Integration software has been installed on their machine, CA DataMinder will create an automatic account name for them that includes their domain, for example unipraxis\frankschaeffer.

Implications for manually created accounts

Because CA DataMinder uses Windows user authentication, this means that if an administrator wants to create a new account for a specific user, the administrator must enter an account name that matches the automatic name that would normally be created for the user when they start up their browser, e-mail application or the Administration console. Typically, this means the administrator must include the domain prefix in the user's account name.

If the administrator omits the domain prefix (for example, frankschaeffer), CA DataMinder will be unable to resolve the new user against the existing accounts when the user next starts up their browser or e-mail application. As a result, CA DataMinder will create a duplicate account name for the user that includes their domain (unipraxis\frankschaeffer), and all captured data will be associated with this account and not the administrator-created account.

More information:

New user Accounts (see page 196)
Central Management Server Settings (see page 188)

Delete Users and Groups

When a CA DataMinder user account is deleted, the user is removed from the User Administration tree. When you delete a group, any users in the group are also deleted.

To delete a user or user group

1. Choose Manage, User Administration or click .
2. Right-click a user or group and choose Delete or click .

Note: The CMS database is updated to show the account is no longer active, but the account itself is not deleted from the database. This enables you to:

- Search for any deleted user accounts using Administration Search.
- Recreate the user at a later date.

Note: You can view a user's group history by clicking the Group History button on the Details tab of the User Properties dialog.

More information:

Recreate Users (see page 198)

Recreate Users

Sometimes it is necessary to recreate a user who was previously deleted. For example, an employee may have left the company and then rejoined at a later date.

When a user account is deleted, CA DataMinder marks that user as deleted, but does not remove their user account from the CA DataMinder enterprise. In practice, this means that the user is no longer visible, and no new events can be associated with them.

If a user is then created with a user name that matches a single deleted user account, CA DataMinder will automatically recreate that deleted user and add an entry to the Activity log. To do this, you need to configure the CMS machine policy to allow user accounts to be undeleted.

When a user is recreated, all user attributes and e-mail addresses are set to their previous values, and links to associated events are restored. All privileges, passwords and management groups are set to the default values for a new user.

More information:

Machine Policy Settings (see page 163)
Add New Users (see page 196)
Central Management Server Settings (see page 188)

User Groups

More information:

Default Group (see page 200)
Set the Default Group (see page 201)
Add New Groups (see page 201)
Move Users Between Groups (see page 202)
Rename Users or Groups (see page 203)

Default Group

Important! When you use CA DataMinder for the first time after installation, we strongly recommend you choose a new default group and define a restrictive policy for this group. This prevents new users from defining their own policy in order to dodge the rules in your organization governing acceptable Web and e-mail usage.

Why is this necessary?

The default group can be any existing user group. It is effectively a holding group until you can move new users into more appropriate groups. But when you use CA DataMinder for the first time, there is only one existing group. This is the 'Users' group and so it is automatically set to be the default group.

Is this a problem? Yes, it is. Of necessity, 'Users' has a non-restrictive policy: no settings are disabled, enforced or hidden. This means any new user who inherits this policy has complete freedom to change any setting in their policy.

To eliminate this problem, you must choose a default group that does have a restrictive policy. That is, key policy settings are enforced, hidden or disabled. This ensures that new users adhere to the rules governing acceptable Web and e-mail usage.

Why does 'Users' have a non-restrictive user policy?

'Users' is always the top level user group in the User Administration tree. By default, it has a non-restrictive user policy. That is, settings are not enforced, disabled, or hidden. This gives you maximum flexibility to selectively restrict policies in child groups lower down the tree.

If you were to redefine the 'Users' policy in order to accommodate new users, for example by enforcing or hiding key settings, these restrictions would cascade down the User Administration tree to affect every user in your organization. This is because you cannot unenforce or unhide settings in the child policy if these restrictive attributes were inherited from its parent policy.

More information:

Set the Default Group (see page 201)

Set the Default Group

To change the default group

New users who create their own CA DataMinder accounts are added automatically to the default group. The default group can be any existing user group. It is effectively a holding group until you can organize new users into more suitable groups.

1. Choose Manage, User Administration or click .
2. Right-click a group and choose Set As Default. The new default group is shown in bold in the User Administration tree.

Note: If an administrator creates a new account for a user, they can assign the user to any existing group.

More information:

Default Group (see page 200)
Add New Users (see page 196)

Add New Groups

There are two ways to add new groups:

To create new groups

1. Choose Manage, User Administration or click .
2. Choose Edit, New Group or click .

To import group from an external source

You can import user groups from an LDAP directory or a CSV file. To do this, use the Account Import wizard.

More information:

New user Accounts (see page 196)
Account Import Overview (see page 37)

Move Users Between Groups

To streamline user administration, you can organize users into hierarchical groups. You can create as many groups as you need. For example, you can create separate groups for each department, and further groups for each team within the department.

Note: You can only move groups if the Allow Groups to be Moved machine policy setting is enabled.

To move users or groups from one group to another

1. Choose Manage, User Administration or click .
2. Either drag-and-drop a user or group onto the new parent group.

   Or right-click a user or group and choose Move Item.

Note: You can view a user's group history by clicking the Group History button on the Details tab of the User Properties dialog.

Important! You need to be aware of the following:

- Moving a user or group can cause unintended changes to their policy!

  Although users and groups normally retain any customized policy settings or attributes when they are moved to a new parent group, it is possible that these will be overwritten if the corresponding settings or attributes inherited from the new parent group are already enforced (for example, or). To avoid such unintended changes, you can configure the Administration console to display a warning before you confirm a move.

- Moving a group can cause unintended row level security issues!

  If a group (and therefore its users) is moved from one parent group to another, the events associated with those users are also 'moved'. Reviewers with rights to the first group lose access to those events, but reviewers with rights to the second group gain access to those events.

  This means that reviewers in the second group can view events associated with users that were not in their management group at the time the event was captured.

  If this is likely to cause a problem, we recommend you leave the Allow Groups to be Moved policy setting at its default setting of False and move users between groups by creating new target groups and moving users as required. This reduces the row level security risk.

More information:

Central Management Server Settings (see page 188)

Rename Users or Groups

To rename users or groups

1. Choose Manage, User Administration or click .
2. Right-click a user or group and choose Rename. But see warning below.

Note: You can view a user's group and full name history by clicking the Group History and Name History buttons (respectively) on the Details tab of the User Properties dialog.

Important! Renaming individual users can be complicated, and depends entirely on how your CMS policy handles new users. You must be especially careful if your CA DataMinder uses Microsoft Windows user authentication to automatically generate new user accounts.

Export the user Hierarchy

You can export the user hierarchy to an XML data file or a command file. This allows you to create an accessible backup of your user hierarchy. It also allows you to edit the exported file to make quick changes to your user hierarchy. You can roll back your user hierarchy, or import the hierarchy changes, by re-importing the exported file using Account Import.

To export a branch of the user hierarchy

1. Click Manage, User Administration.

   The user hierarchy displays in the navigation pane.
2. Right-click a group and click Export Hierarchy to File.

   The Export Hierarchy to File dialog appears.
3. Specify the file name and location.

4. Specify the export file format:

   XML Data File

   Exporting to an XML file allows you to edit the user hierarchy quickly using an XML editor.

   Command File

   If you export to a command file, we recommend that you do not re-import the command file back onto your working CMS using Account Import. Each line in the exported file is a command (for example, *newutility*, *newuser* or *newgroup*) to add data to the CMS database, but that data already exists. If you re-import this command file, CA DataMinder logs these commands as warnings in the Account Import log file.

5. (Optional) If any groups or users have names that contain Far Eastern characters, select the Unicode check box. You must export in Unicode format to preserve these characters in the exported file.

6. Specify which user details to export. You can export user roles, management groups, attributes and e-mail addresses.

More information:

Account Import Overview (see page 37)

User Properties

For individual users, you can set up names and roles and assign administrative privileges. These privileges determine the features available to users in the Administration console. You can also modify and update users' attributes and e-mail addresses.

To set user properties

1. Right-click a user and choose Properties.

2. In the User Properties dialog, edit properties in the following tabs:

   Details tab

   Set the names and password for an individual user, plus their group, management group, user role, and security model.

   Privileges tab

   Assign or revoke a user's administrative privileges. These determine what a user is permitted to do when using CA DataMinder consoles.

Addresses tab

Update the e-mail addresses associated with the current user.

Attributes tab

Update the user's attributes. For example, your CA DataMinder user accounts have Department and Telephone Number attributes.

More information:

Privileges (see page 205)
Passwords (see page 211)
Security Models (see page 211)
Policy Roles (see page 218)
User Roles (see page 220)
Management Groups (see page 226)
Addresses (see page 227)
Attributes (see page 228)

Privileges

Administrative privileges determine the features available to users in CA DataMinder consoles:

- *Admin privileges* permit a user to perform administrative tasks such as redefining user roles or disabling management group filtering.
- *Audit privileges* determine which event auditing tasks are available to a reviewer in the iConsole.
- Event privileges control event handling. For example, they permit reviewers to run event searches, import or export events, or change event expiry dates.
- *Machine privileges* permit administrators to manage the CA DataMinder machine hierarchy and view log files.
- *Policy privileges* permit policy administrators to view and edit CA DataMinder policies.
- *User privileges* permit administrators to manage the user hierarchy and reset passwords.

To assign administrative privileges

1. Right-click a user and click Properties.
2. In the User Properties dialog, click the Privileges tab.
3. Select the privileges (see page 206) you want to assign to the current user.

   Note: User roles provide a shortcut method for assigning administrative privileges. You can also change the default set of privileges assigned to each role.

More information:

What Administrative Privileges Are Available? (see page 206)

What Administrative Privileges Are Available?

CA DataMinder supports the following administrative privileges:

Admin: Allow administration searches

Allows a user to search for user, group or machine accounts in the Administration console.

Admin: Allow iConsole dashboard searches

Allows a user to view dashboards in the iConsole.

Admin: Allow unrestricted SQL searches

Allows a user to edit the raw SQL search expression generated in the SQL tab when searching for administration data or captured data. Without this privilege, users can view but cannot edit the SQL tab. All administrators get this privilege automatically.

Important! Because this privilege permits users to write unrestricted SQL queries, we strongly recommend that it is granted to other user roles only when absolutely necessary.

Admin: Assign undefined privileges

Allows a user to acquire any new privilege added to CA DataMinder after an upgrade. Only the primary administrator and users with the administrator role get this privilege automatically.

Important! Because this privilege assigns potentially unknown privileges, we strongly recommend that it is granted to other users only when absolutely necessary.

Admin: Disable security model filtering

Allows a user to bypass security restrictions and search for events outside of their management group. It also enables a user to search for events that are not associated with a CA DataMinder user. Only users with the administrator role get this privilege automatically.

Important! Because this privilege permits users to bypass security, we strongly recommend that it is granted to users only when absolutely necessary.

Admin: Edit customizable console text

Allows a user to define audit status descriptions and customized user attributes.

Admin: Edit user roles

Allows a user to add new user roles and to modify the default set of administrative privileges assigned to each user role.

Admin: Install license file

Allows a user to install a license file on the CMS. The license file determines which policy modules are available in your CA DataMinder installation.

Admin: Manage System Files

Allows a user to view or edit system files on the CMS using the System File Explorer. For example, users can install a new definition file for US Social Security numbers.

Admin: Manage iConsole

Allows a user to access the Administration tab in the iConsole. This tab enables users to manage searches and reports and to define custom iConsole configurations for user roles. For example, this privilege permits a user to install and publish a new search and to specify which user roles can run the new search. This privilege also allows a user to define the default layout for the home page.

Typically, only administrators have this privilege.

Admin: Manage security models

Allows a user to add, modify or remove security models. This also allows a user to set the database credentials for each security model (these are the database accounts that CA DataMinder uses to access the CMS database).

This privilege also lets users set the password for the database primary user (by default, WGNUSER).

Note: This privilege is not connected to the 'Users: Reset user passwords' privilege; see below.

Admin: Use single sign-on

Allows a user to log on with single sign-on, even if the CMS machine policy setting Allow single sign-on? is set to False.

Agents: Edit content agents

Allows a user to set up registered content agents.

If a user has neither this privilege nor View content agents (see below), the Registered Content Agents branch is hidden from the user in the Administration console.

Note: This privilege does not affect an administrator's ability to configure Content Agent triggers.

Agents: View content agents

Allows a user to view registered content agent details.

Note: This privilege does not affect an administrator's ability to configure Content Agent triggers.

Audit: Allow auditing without viewing the event

Allows a user to change the audit status of an event without needing to view it. This also makes it possible to change the audit status of multiple events in a single operation.

Audit: Always suppress automatic auditing

Allows a user to view events without adding a Viewed Event entry to the audit trail. Other audit activities, such as changing an event status or forwarding a copy of the event via email will create an audit entry.

Audit: Always suppress automatic export logging

Allows a user to export events (to either a self-contained web site, or a Microsoft Personal Folder) without adding a Exported Event entry to the audit trail.

Audit: Choose to suppress automatic auditing

Allows a user to choose whether to view events without adding a Viewed Event entry to the audit trail. The user is prompted to choose when opening the first event of a new search and that choice stands for all events in the current search results. If the same search is rerun, the user is prompted again.

Note: For full access to auditing features in the Audit tab, the user also needs the Audit: Update audit trail privilege - see below.

Audit: Update audit trail

Allows a user to update the audit trail for an individual event.

Audit: View audit trail

Allows a user to view, but not update, the audit trail for an individual event.

Events: Allow bulk session management

Allows a user to access multiple CA DataMinder user accounts.

Events: Allow content searches

Allows a user to search for captured web and email documents based on their text content. Content searches look for documents saved and indexed in a CA DataMinder content database. They are available in the iConsole and Data Management console.

Events: Allow download of original content

Allows a user to download an event in its original format, such as MSG files for email message.

Events: Allow event import

Allows a user to run the Event Import utility.

Events: Allow event searches

Allows a user to search for captured web, email and application data in the iConsole and Data Management console.

Events: Allow export

Allows a user to export search results to either a self-contained web site, or a Microsoft Personal Folder (PST file).

Events: Allow searches of unlimited size

Allows an iConsole reviewer to run 'unlimited' event searches. That is, the iConsole will return all events that match the search criteria, disregarding any result limits defined in the registry.

Note: For this privilege to take effect, the iConsole must be configured for unlimited searches. For details, see the *Platform Deployment Guide*; search the index for 'iConsole: search results, configuring'.

Events: Change expiry dates

Allows a reviewer to edit the expiry date and 'do not delete' flag for an event.

Events: Control quarantined events

Allows a user to either release or reject an email from quarantine.

Events: View captured data

Allows a user to view captured data associated with any user in their management group. This privilege also allows users to use the Content Indexer utility (a necessary task before using content agents or running content searches).

Events: View expiry dates

Allows a user to view the expiry date and 'do not delete' flag for an event.

Machines: Edit the machine hierarchy

Allows a user to manage machine accounts in the Machine Administration screen.

Note: This privilege also permits users to suspend and resume machines.

Machines: View log files

Allows a user to access the Log Files screen.

Machines: View the machine hierarchy

Allows a user to view existing machine accounts in the Machine Administration screen.

Policies: Edit policy

Allows a user to view and edit any machine policy and any user policy that falls within their management group.

Policies: Edit the CMS policy

Allows a user to edit the machine policy for the CMS. If you clear this check box, access to the CMS policy is denied but users can still edit other machine policies.

Policies: Replicate changes to clients

Allows a user to replicate any policy changes down to client machines immediately. If a user does not have this privilege, any changes they make will replicate automatically at intervals defined in the CMS policy.

Policies: View policy

Allows a user to view any machine policy and any user policy that falls within their management group.

Users: Edit the user hierarchy

Allows a user to access the User Administration screen and manage accounts for any user in their management group.

Users: Reset user passwords

Allows a user to set a new CA DataMinder password for another user without knowing their existing password.

Note: This privilege does not apply to database logon passwords. These are governed by the Admin: Manage Security Models privilege - see above.

Users: View the user hierarchy

Allows a user to access the User Administration screen and view accounts for any user in their management group.

Passwords

Note that you cannot set blank passwords. This is a security precaution to prevent unauthorized access to your store of captured data on the CMS.

To change your own password

Choose File, Change Password.

To change another person's password

1. Right-click a user and choose Properties.
2. In the User Properties dialog, click the Details tab.
3. Click Set Password.

   Note: After setting or changing a password, there will be a short delay before the user can log in using the new credentials. This is because the new password must first be replicated to the user's console machine. The replication frequency for infrastructure changes is controlled by the machine policy.

Security Models

Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database.

You can choose which security models are available on your CMS. You can also have multiple security models active at the same time, though each reviewer is linked to a single model.

For example, some reviewers may only be permitted to see events linked to users in their own management group. Other reviewers may only be permitted to see specific types or categories of events.

CA DataMinder supports the following security models:

Management Group (Standard)

This is the default model, optimized to allow fast searching. It is based on the CA DataMinder user hierarchy.

It uses e-mail addresses (including synthesized addresses for participants in Web and Application Monitor events) to map participants to CA DataMinder users. Under this model, reviewers can only view events where at least one participant was in their management group when the event was captured.

You can also include this model in a hybrid with a Policy model (see below).

Management Group (Standard, Self-Exclude)

This model prevents reviewers from seeing their own events. As above, reviewers can only view events where at least one participant was in their management group. However, under this model the search results also exclude any events in which the 'logged-on user' (that is, the reviewer) was a participant.

You can also include this model in a hybrid with a Policy model (see below).

Management Group (Sender)

Under this model, when a reviewer runs an e-mail search, they can only view events where the e-mail sender was in their management group when the event was captured.

Important! This sender-centric security model is only appropriate for e-mail searches. Searches for other event types will return zero results.

You can also include this model in a hybrid with a Policy model (see below).

Management Group (Sender, Self-Exclude)

This model prevents reviewers from seeing their own e-mails (or any other events) when they run a search.

As above, reviewers can only view events where the e-mail sender was in their management group. However, under this model the search results also exclude any events in which the 'logged-on user' (that is, the reviewer) was a participant.

You can also include this model in a hybrid with a Policy model (see below).

Policy (Standard)

This model ensures that reviewers can only see specific types of event. For example, this model can be used to ensure that HR reviewers only see events that relate to HR issues such as employee behavior, while Legal reviewers only see events that relate to legal issues such as litigation threats or a breach of attorney client privilege.

The model is based on *policy classes*. For categorization purposes, you can associate individual triggers with a *policy class*, such as 'Employee Behavior' or 'Legal'. When a trigger fires, the policy class is stored with the associated event.

Likewise, each reviewer has a policy role. A *policy role* links a user to a collection of policy classes. In effect, the policy role determines which policy classes a user is permitted to see. When the user runs a search, the results only include events associated with these policy classes.

Before using this security model, you must define policy classes for triggers in your user policies, define your policy roles, and assign policy roles to your reviewers.

- Policy classes are described in the *Policy Guide*.
- Policy roles (see page 218) are described in the *Administration Guide*.

You can also include this model in a hybrid with a Management Group model (see below).

Policy (Standard, Self-Exclude)

This variant of the Policy model prevents reviewers from seeing their own events. As above, reviewers can see only specific types of event. However, the search results also exclude any events in which the reviewer was a participant

Before using this security model, you must define policy classes for triggers in your user policies, define your policy roles, and assign policy roles to your reviewers.

You can also include this model in a hybrid with a Management Group model (see below).

Policy (All Events, Restricted Triggers)

This variant of the Policy model allows reviewers to see any events in the CMS database when they run a search. That is, no events are excluded from the search results.

However, the reviewer can only see trigger and audit details for events covered by their policy role. Specifically, the Search Results screen only shows trigger and audit details for events associated with policy classes in the reviewer's policy role. If the search results include events associated with other policy classes, trigger and audit details for these events are hidden in the Search Results screen.

Before using this security model, you must define policy classes for triggers in your user policies, define your policy roles, and assign policy roles to your reviewers.

You can also include this model in a hybrid with a Management Group model (see below).

Hybrid Models: Management Group and Policy

If required, you can add a hybrid model on your CMS. This combines the Management Group and Policy models. Its effect is to restrict reviewers so they can only see specific types of event associated with users in their management group. For example, under this model a reviewer in the Legal team can only review legal events associated with members of their management group.

You can create hybrid models from any Management Group variant and any Policy variant. For example, you can create a hybrid from the 'Management Group (Self Exclude)' and the 'Policy (All Events, Restricted Triggers)' models. Here, a reviewer can only see events associated with users in their management group. But they cannot see events in which they were themself a participant and they cannot see trigger and audit details for events not covered by their policy role.

Before using this security model, you must define policy classes for triggers in your user policies, define your policy roles, and assign policy roles to your reviewers.

Unrestricted

This model is not subject to row level security (RLS). It permits reviewers to see any database items (events, users, triggers, and so on) when they run a database query. For example, Search results or reports are not restricted by policy class or the reviewer's management group. This model is required by:

- CA DataMinder administrators. Paradoxically, this security model *restricts* the extent to which administrators can edit the CMS database. Specifically, it prevents administrators from inadvertently updating the CMS database when they exercise their 'Admin: Allow Unrestricted SQL Searches' privilege.
- CA DataMinder user accounts set up explicitly for use by external reporting tools *that require full access* when searching the Data Warehouse for events.

  Note: If the user of an external reporting tool is subject to row level security, CA DataMinder applies that user's security model (typically a Management Group model) when the user runs a report.

Note: You can only assign the Unrestricted security model to a CA DataMinder user if you have the 'Admin: Disable security model filtering' administrative privilege.

Important! Certain reports and the Review Queue are not designed for use with Policy security models. See the reference below for details.

More information:

Default Security Model (see page 215)
Manage Security Models (see page 216)
Assign a Security Model to a User (see page 217)
Policy Security Models Not Compatible With Some Reports or Review Queue (see page 218)
Security Model Limitations for Content Searches (see page 218)

Default Security Model

When you first install CA DataMinder, only one security model is active. This is the default security model, Management Group (Standard). Note the following:

Users are automatically assigned to default security model

When a CA DataMinder user account is first created, the user is automatically assigned to the default model. (Technically, the user is assigned to the default user role, which in turn assigns the default security model to the user).

If you subsequently make other security models active on your CMS, you can link the user to a different model.

If you remove a non-default security model, any reviewers still assigned to this model will revert to the default security model.

The default security model can be modified

If required, you can change the model type. For example, you can change the default model to Policy (Standard) or Management Group (Standard, Self-exclude).

If you change the model type, its name as shown in the Administration console will change accordingly.

The default security model cannot be removed

Unlike other security models active on your CMS, you cannot remove the default security model.

User roles have default security models

Each user role has its own 'default security model'. Each user assigned to the role inherits this model.

This can be any security model active on the CMS, and can be different to the actual default security model.

Administrator role uses the Unrestricted security model

By default, the Administrator role uses the Unrestricted security model. Users assigned to this security model have no management group.

Consequently, administrators have no management group and their administrative authority extends to all users. An administrator's authority is *not* restricted to specific user groups.

Manage Security Models

Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database for events.

CA DataMinder supports multiple security models, including models based on management groups, variants of this original model (for example, to prevent reviewers reviewing their own e-mails), and policy-based models. You can choose which models are active on your CMS and multiple models can be active at the same time. However, each reviewer can only be linked to a single model. For example, some reviewers may only be permitted to see events linked to users in their own management group. Other reviewers may only be to see specific types or categories of events.

When you first install CA DataMinder, only one security model is active. This is the default security model, Management Group (Standard). You must enable other security models before you can assign them to reviewers.

Important! CA DataMinder administrators require the Unrestricted security model. You *must* enable this model before you assign users accounts to the Administrator role.

You can manage security models in the Administration console.

To enable a security model on the CMS

1. Choose Tools, Manage Security Models.
2. In the Manage Security Models dialog, click Add.

   The Create Security Model dialog displays.
3. Set the Database User Name. CA DataMinder consoles use this database account to connect to the CMS database when searching for events under the new security model.

   a. Click the Set Credentials button.

   b. In the Set Model Credentials dialog, enter the name and password for a secure database account.

   Important! Each security model must use its own database account. Security models cannot share the same database account.
4. Choose the Model Type from the available types, such as Management Group (Sender).
5. (Optional) Create a hybrid security model. This combines two security models to filter the results when a reviewer searches for events.

   a. Select the Hybrid Model Type check box.

   b. Choose the second security frmo the available types.
6. Click OK.

To modify a security model

1. Choose Tools, Manage Security Models.
2. Select model you want and click Modify.

   You can now change the database user name or model type.

To remove a security model

1. Choose Tools, Manage Security Models.
2. Select model you want and click Remove.

   Any reviewers still assigned to this model will revert to the default security model. (Typically, this is the Management Group (Standard) model, although you can change the default model type.)

More information:

Security Models (see page 60)

Assign a Security Model to a User

Each CA DataMinder reviewer must be assigned to a database security model. Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database for events.

Note: Before you can assign security models to users, you must enable the models you want on your CMS.

To assign a security model to a user

1. Right-click a user and choose Properties.
2. In the User Properties dialog, go to the Details tab.
3. Choose a model from the Security Model list.

   Note: You can only assign the Unrestricted security model to a CA DataMinder user if you have the 'Admin: Disable security model filtering' administrative privilege.

More information:

Manage Security Models (see page 33)

Policy Security Models Not Compatible With Some Reports or Review Queue

Certain reports, particularly the compliance reports such the Repeat Offender report and Compliance Audit Report, are not designed for use with Policy security models. This is also true for the Review Queue feature and the associated Reviewer search.

These reports and the Review Queue are explicitly designed to be run in conjunction with the Management Group security models. That is, they return data about users in specific user groups.

Important! We recommend that any users who need to run these reports or the Reviewer search are assigned to a Management Group security model, not to a Policy security model.

Security Model Limitations for Content Searches

Content searches only support the Management Group security model. If a reviewer has a different security model and runs a content search, the search returns zero events.

Also, unlike the Standard Search, if a reviewer has the top-level 'Users' group as their management group, a content search may return events where no participants map to CA DataMinder users. However, if a reviewer tries to view such events in the iConsole or Data Management console, CA DataMinder blocks access to these events.

Policy Roles

You can use policy roles to ensure that a user can only see events captured by specific types of trigger when they search for events.

For categorization purposes, you can associate individual triggers with a *policy class*, such as ‘Employee Behavior’ or ‘Legal’. When a trigger fires, the policy class is stored with the associated event.

A *policy role* links a user to a collection of policy classes. In effect, the policy role determines which policy classes a user is permitted to see. When the user runs a search, the results only include events associated with these policy classes.

Manage Policy Roles

Each policy role is associated with a set of specific policy classes and individual policies. You can define as many policy roles as you need.

To add a role

1. In the Administration console, click Tools, Manage Policy Roles.
2. In the Manage Policy Roles dialog, click Add to define a new policy role.

To modify a role

1. In the Administration console, click Tools, Manage Policy Roles.
2. Select a policy role and click Modify.
3. In the Policy Role dialog, choose the policy classes or individual policies that you want to associate with the policy role.

To remove a role

1. In the Administration console, click Tools, Manage Policy Roles.
2. Select a policy role and click Remove.

Important! If you remove a policy role while users are still assigned to it, these users will have no policy role. Consequently, they will be unable to view **any** events in the iConsole until you reassign a policy role to them!

Assign a Policy Role

You can assign a policy role to a user role to control which types of events the users can see. You can also assign policy roles to individual users.

To assign a policy role to a user role

1. Click Tools, Manage User Roles.

   The Manage User Roles dialog displays.
2. Click a user role.
3. Verify that the Default Security Model for the user role is a policy-based security model, such as 'Policy (Standard)'.

   Note: You can only assign a policy role if the user role is already assigned to a policy-based security model.
4. Choose a policy role from the Default Policy Role list.

To assign a policy role to an individual user

By default, an individual user inherits the policy role associated with their user role. But you can assign a different policy role to users.

1. Right-click a user and choose Properties.

   Note: You can only assign a policy role if the user is already assigned to a policy-based security model.

2. In the User Properties dialog, go to the Details tab.
3. Choose a policy-based model from the Security Model list.
4. Choose a policy role from the Policy Role list.

More information:

Manage Security Models (see page 33)

User Roles

Each user in CA DataMinder is assigned to a user role, for example, Administrator, Manager, or User. The user role determines the default set of administrative privileges assigned to the user and their security model.

Administrative privileges determine the features available to users when using CA DataMinder consoles. Security models ensure that reviewers can only see events they are permitted to see when searching the CMS database.

More information:

Default User Roles (see page 221)
Configure the Specialist Reviewer Roles (see page 222)
Manage User Roles (see page 223)
Assign a User Role (see page 224)
Reassign Users with 'Custom' Roles to Existing User Roles (see page 225)
iConsole Configuration Based on User Roles (see page 225)

Default User Roles

The default user roles are listed below. You can also create your own custom roles.

Administrator

These administer your CA DataMinder installation. By default, these have the full range of privileges.

Note: If future versions of CA DataMinder introduce new privileges, these will be granted automatically to all users with an Administrator role when you run the upgrade.

Manager

These users manage your organization. Their privileges focus on searching for captured data.

Policy Administrator

These users are permitted to view and edit policies, but not to manage user or machine accounts or search for captured data.

Reviewer

These users have the same privileges as Managers but can also view and edit the audit status of captured events.

Security Reviewer, PCI Compliance Reviewer, Human Resources Reviewer, Compliance Reviewer

These specialist user roles have the same privileges as an ordinary Reviewer, but they are each associated with a specific *policy role.* This means that the reviewer can only see specific types of events in the iConsole or Data Mangement console.

For example, the PCI Compliance Reviewer user role restricts reviewers so that they can only see events that breached your policies on the handling of payment card information. (This user role is associated with the 'PCI Compliance Policies' policy role, which in turn is based on the Credit Card Information policies in the PII policy class.)

Likewise, users with the Human Resources Reviewer role can only see events that breached Employee Behavior policies.

Note: You must configure these reviewer roles (see page 222) before you can assign them to users.

System Process

This user role is reserved for the NT_AUTHORITY\SYSTEM and Quarantine Manager user accounts. Do not assign this role to real users.

The NT_AUTHORITY\SYSTEM account is created automatically when you install the CMS.

The Quarantine Manager account is a CA DataMinder account that operates in conjunction with the QM domain user. For details, see the Quarantine Manager chapter in the *Platform Deployment Guide*.

User

These users are ordinary CA DataMinder users with no administrative privileges.

UserRole1 and UserRole2

These are existing custom roles that you can customize to suit the needs of your organization.

More information:

User Properties (see page 204)

Configure the Specialist Reviewer Roles

CA DataMinder supports the following specialist reviewer user roles:

- Compliance Reviewer
- Human Resources Reviewer
- PCI Compliance Reviewer
- Security Reviewer

Before you can assign users to these roles, you must configure the roles to use an appropriate policy class.

How to configure a Specialist Reviewer Role

1. Enable a Policy security model.
2. Assign the Policy security model to one of the reviewer user roles.

   For example, assign the Policy (standard) security model to the 'PCI Compliance Reviewer' user role.
3. Assign the appropriate policy role to the reviewer user role.

   For example, assign the 'PCI Compliance Policies' policy role to the 'PCI Compliance Reviewer' user role.
4. Customize the iConsole for the reviewer user role.

   For example, you can specify which settings, portlets, searches, and reports are available to these reviewers when they use the iConsole. For details, see the 'iConsole Administration' chapter in the *iConsole User Guide*.

See the references below for detailed instructions.

More information:

Manage Security Models (see page 33)
Assign a Security Model to a User (see page 217)

Manage User Roles

Each user in CA DataMinder is assigned to a user role, for example, Administrator, Manager, or User. The user role determines the default set of administrative privileges assigned to the user and their security model.

You can redefine, rename and create user roles if you have the Admin: Edit user roles privilege.

If you change the default set of privileges assigned to a user role, CA DataMinder automatically updates the privileges of all users in that role. For example, if you add a privilege to the Manager role, all users in the Manager role are automatically granted the new privilege.

Note: If future versions of CA DataMinder introduce new privileges to a default role, these privileges are granted automatically to all users assigned to that role when you upgrade CA DataMinder.

To redefine a role

1. Click Tools, Manage User Roles.
2. In the Manage User Roles dialog, select the role that you want to edit.
3. If required, you can:
   - Rename the role.
   - Assign or remove administrative privileges.
   - Set the default security model.
   - Set the default policy model.

To create a new role

1. Click Tools, Manage User Roles.
2. Click New to display the Create New User Role dialog.
   a. Enter a name for the new role.
   b. Specify which existing role you want to copy from.

      The administrative privileges assigned to the existing role are copied to the new role.
   c. Click OK to close the dialog.

      The new user role is created.
3. If required, modify the administrative privileges and default security model assigned to the new role.

Assign a User Role

You can assign a user role to a user in order to control which CA DataMinder features and actions are available to that user. When users are assigned to a user role, they automatically inherit the default administrative privileges for that role.

To assign a user role to a user

1. Right-click a user and click Properties.
2. In the User Properties dialog, go to the Details tab.
3. Click Change User Role and select the new role.

   Note: After assigning a user role, you cannot change the administrative privileges assigned to that user. If an individual user requires a custom set of privileges, you must create a new user role and assign the required privileges to that new role. Then assign the role to the user.

Reassign Users with 'Custom' Roles to Existing User Roles

In previous releases, the administrative privileges assigned to an individual user derived from that user's User Category (such as Manager or Reviewer). However, it was also possible to assign a custom set of administrative privileges to an individual user. Such users were automatically assigned to a 'Custom' user category.

In the current version of CA DataMinder, you cannot directly change a user's privileges. As a result, it is no longer possible to create a 'Custom' user role. Instead, you can only change a user's privileges by reassigning the user to a different user role. This change has been introduced to support role-based iConsole configuration. Briefly, you can now specify which iConsole features (portlets, searches, and so on) are available to users with specific user roles.

If you upgrade from a previous version of CA DataMinder, any existing user assigned to a custom role retains this custom role in the current version of CA DataMinder. However, such custom user roles are not supported in the iConsole. In particular, you cannot specify which features are available to users with custom roles when they use the iConsole. In this situation, we recommend that you assign users without a recognized role to an equivalent 'official' user role. Do one of the following:

- Manually reassign users with a custom role to one of the default user roles.
- Add new user roles that correspond to the various custom roles held by your users. Then reassign these users to the new user roles. CA DataMinder provides a 'CustomRoleUpgrade' utility that automates this process.

  For instructions, search for 'CustomRoleUtility' in the *Upgrade Guide*.

iConsole Configuration Based on User Roles

You can configure the iConsole separately for different user roles. For each role, you can specify which settings, portlets, searches, and reports are available to users when they use the iConsole.

For example, an administrator has added two new user roles, HR Reviewers and PII Reviewers. In the iConsole, the administrator can assign separate searches to each role. The searches available to HR Reviewers focus on emails captured by Employee Behavior policies in the standard policy pack. Conversely, searches available to PII Reviewers focus on emails captured by Personally Identifiable Information policies.

Likewise, you can configure iConsole settings and portlets to allow Administrators to define their own personal home pages but prevent other users from doing so.

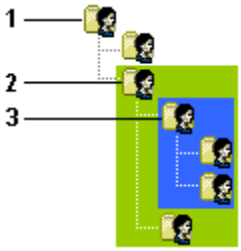
Instructions for setting up role-based iConsole configurations are in the *iConsole User Guide* and iConsole online help.

Management Groups

A management group determines which groups and subgroups an administrator is permitted to manage. For a reviewer, their management group limits any search results to include only events associated with users in this group.

A management group is the highest level group in any branch of the user hierarchy that they are permitted to manage. If required, an administrator can have multiple management groups.You can assign any existing group as a management group for a particular administrator. Assigning multiple management groups enables an administrator to manage separate branches of the user hierarchy.

Each management group represents a ‘management branch’ of the user hierarchy. Within each management branch, an administrator can manage user accounts, edit policies, view captured data and so on. Any groups that lie outside this branch are hidden in the console, and cannot be managed by the administrator. In the example below, if the administrator is assigned to management group 3, he or she cannot view data captured on behalf of users in a green group.



If the management group is:

1, the administrator can manage any group in the organization.

2, the administrator can manage the green and blue groups.

3, the administrator can manage the blue groups only.

To assign a management group

1. Right-click a user and choose Properties.

   Note: You cannot set or change the management group of a user who has the 'Admin: Disable security model filtering' privilege.

2. In the User Properties dialog, go to the Details tab.
3. Go to the Management Group section and click the Browse button.
4. In the resulting dialog, select the group you want.

To override management group constraints

You can permit an administrator to bypass management group security measures and search for events throughout the entire CA DataMinder enterprise.

1. Right-click the user you want and choose Properties.
2. In the User Properties dialog, go to the Privileges tab.
3. Grant the 'Admin: Disable security model filtering' privilege.

Addresses

Important! It is critical that user e-mail addresses are kept up to date. This is because key CA DataMinder features (Event Import, policy engines and User Attribute lookup) rely on e-mail address mapping to associate e-mails with specific CA DataMinder users. For details on synchronizing user e-mail addresses in the CMS database with addresses in an external source (for example, Active Directory), see the *Platform Deployment Guide*; search for 'Account Import'.

You can associate multiple e-mail addresses with a single CA DataMinder user. This tab enables you to add or modify e-mail addresses for the current user. It is important to keep these addresses up to date as many CA DataMinder features reference them.

To update user e-mail addresses

1. In the Administration console, right-click a user and choose Properties.
2. In the User Properties dialog, go to the Addresses tab.
3. Use the Add, Remove and Modify buttons to update the address list for the current user.

Attributes

CA DataMinder lets you define attributes for your CA DataMinder user accounts. For example, you can create an Employee ID attribute and assign a unique ID to each user in your organization.

To create a custom attribute

To create custom attributes for users in your organization, you must rename one of the default attributes.

1. Choose Tools, Options.
2. In the Options dialog, go to the User Attributes tab.
3. Select an existing attribute and click Modify.
4. Enter the new attribute name.

To update a user's attributes

1. Right-click a user and choose Properties.

   Note: You cannot change your own attributes.
2. In the User Properties dialog, go to the Attributes tab.
3. Use the Add, Remove and Modify buttons to update the attribute values.

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

Account Import

More information:

Account Import Overview (see page 231)
Synchronize E-mail Addresses (see page 231)
Import Methods and Sources (see page 232)
Handling for Unknown Users (see page 233)
Multiple attribute Values (see page 234)
Modify LDAP Values with Conversion Expressions (see page 234)
Automatically Exempt Users From Policy (see page 235)
Account Import Log Files (see page 235)

Account Import Overview

To simplify mass deployments, you can use the Account Import feature to import user details into CA DataMinder from an external Lightweight Directory Access Protocol (LDAP) directory or a source file. Account Import can:

- Import new users and groups into the existing CA DataMinder user hierarchy.
- Reorganize existing CA DataMinder users to synchronize them with an external user hierarchy, for example, an LDAP directory structure.
- Create new CA DataMinder accounts for unknown users. These are imported users who have no corresponding account in CA DataMinder.
- Add a domain as a prefix to all imported user account names, such as unipraxis\frankschaeffer.
- Update CA DataMinder user accounts with imported attributes such as e-mail addresses and employee IDs.
- Exempt specific users from policy. CA DataMinder can exempt users with specific LDAP Attributes or, if you import from an XML data file, users with the *policyexempt* attribute.

Note: For full details about user import operations, see the *Platform Deployment Guide*; search for 'Account Import'.

Synchronize E-mail Addresses

Important! One of the most important uses for Account Import is to synchronize users' e-mail addresses in the CMS database with addresses in an external source, typically an LDAP directory such as Active Directory.

Such synchronization is essential for CA DataMinder features that rely on e-mail address mapping:

- Policy engines
- User attribute data lookup
- Event Import

For full details about e-mail address mapping and importing e-mail addresses, see the *Platform Deployment Guide.* Search for 'e-mail address mapping' and 'account import'.

More information:

Account Import (see page 230)

Import Methods and Sources

Account Import can import user details from several sources, and supports two import methods:

Import methods

You can import user details by running:

Account Import wizard

This is the simplest method for importing user details. You launch the wizard from the Administration console: choose Tools > Account Import Wizard. The wizard can import data from any supported source—see the next section.

Command line import operations

These enable you to schedule regular import operations, for example, to ensure that your LDAP directory and CA DataMinder user hierarchy stay synchronized. From a command line, you can import data from any supported source—see the next section.

Import sources

Account import can import user information directly from an LDAP directory, data file or command file:

LDAP directory

The Lightweight Directory Access Protocol (LDAP) enables directory services to manage directory objects. Objects and attributes in an LDAP directory are exposed to any other application that uses the LDAP protocol. CA DataMinder can import user details from the following LDAP directories:

- Microsoft Active Directory
- Novell eDirectory (NDS)
- Netscape/Sun ONE Directory Server
- Domino Server 6.0.4, 6.5, or 7.x

Data files

These are structured files of user data, in XML or spreadsheet-compatible format. Data files contain encoded versions of all or part of an external user hierarchy and contain the user details necessary for CA DataMinder to create, or re-create, this external hierarchy on the CMS.

Command files

These are import configuration files containing CA DataMinder user and machine import commands (for example, 'create new user' or 'set user attribute'). Typically, you import command files to make specific changes or additions to your existing CA DataMinder user hierarchy.

Note: For full details about user import operations, see the Account Import chapter in the *Platform Deployment Guide*.

More information:

Account Import (see page 230)

Handling for Unknown Users

When you import users from an LDAP directory, you can specify how CA DataMinder handles 'unknown' users or groups. These are users and groups in your existing CA DataMinder user hierarchy that are not present in the LDAP directory or XML data file.

Specifically, you can move unknown users to an 'exceptions' group and you can exempt them from policy.

Exempt from policy

You can exempt unknown users from policy.

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.

'Exceptions' group

The exceptiopns This can be any existing group that falls within your management group. However, be aware that this reorganization only affects CA DataMinder users within the specified parent group. Unknown users outside of this branch of the user hierarchy are not reorganized.

The following example specifies the Management group as the destination for imported users. If required you can move any unknown users within this group or its subgroups to an exceptions group. However, any unknown users outside of this group or its subgroups are not reorganized. For example, unknown users in the Sales group are not reorganized into the exceptions group.

Example CA DataMinder user hierarchy

The Management group is the target parent group for imported users. Unknown users in the Marketing and Sales groups are not reorganized.

More information:

Account Import (see page 230)

Multiple attribute Values

Individual attributes in both CA DataMinder and LDAP directories can contain multiple values. This has implications for user import operations from an LDAP directory.

Importing a single LDAP attribute with multiple values

Individual attributes in LDAP directories can contain multiple values. For example, a MemberOf attribute can contain all the mail groups or e-mail distribution lists that a user belongs to.

Account Import automatically writes multiple LDAP values to multiple values of a specific CA DataMinder user attribute. For example, you can import all the MemberOf distribution lists that a CA DataMinder user belongs to as separate values for an attribute renamed to Email Distribution Lists.

Combining multiple LDAP attributes in single CA DataMinder attributes

If necessary, Account Import can write multiple LDAP attributes to a single attribute of a CA DataMinder user account. For example, the LDAP directory may contain three attributes, Building, Floor and Desk number. Using Account Import, you can combine these attributes into a single value and write this value to a single CA DataMinder user attribute renamed to Desk Location.

More information:

Account Import (see page 230)

Modify LDAP Values with Conversion Expressions

A key feature of command line import operations from LDAP is the ability to modify user attribute values in the LDAP directory before writing them to an attribute of a CA DataMinder user account. Conversion expressions can parse, extract and (if necessary) remove or substitute any characters in the attribute value.

To modify imported LDAP values, you configure the /al or /ml parameter to use a conversion expression. For example, if importing e-mail addresses from the proxyAddresses LDAP attribute, e-mails addresses are typically prefixed with a format identifier (such as 'smtp:' or 'x500'). Account Import uses default conversion expressions to strip out these identifiers so that only the address is imported into CA DataMinder:

```
["smtp:{%untilEnd%}"]
["x400:{%untilEnd%}"]
["x500:{%untilEnd%}"]
```

For full details about conversion expressions, please refer to the *Platform Deployment Guide*; search for 'Account Import'.

More information:

Account Import (see page 230)

Automatically Exempt Users From Policy

Account Import can automatically exempt users from policy.

If you use the Account Import wizard to import user details, you enter exemption details in the Sychronization Scope wizard screen. For example, you can specify the LDAP attribute that exempts an imported user from policy.

For command line import operations, Account Import jobs support policy exemption commands and parameters.

For full details, see the Account Import chapter in the *Platform Deployment Guide*.

Account Import Log Files

The results of each individual import operation are written to a separate logfile. To view the logfile, choose Manage, Logfiles or click .

The logfile lists all changes or additions to the existing CA DataMinder user or machine hierarchies. It also includes any errors that may have occurred. For example, if the wizard failed to find a specified parent group or parent server this is recorded in the logfile.

Note: You can only view logfiles if you have been granted the View Logfile administrative privilege.

More information:

Account Import (see page 230)
Import or Reparent Machines (see page 129)

Chapter 13: User Policies

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.

This section briefly describes how to administer user policies in the Adminstration console. For full details about configuring user policies to protect your data, see the *Policy Guide*.

This section contains the following topics:

What is in a User Policy? (see page 238)
Policy Versions (see page 238)
User Policy Editor (see page 242)
Edit a Policy (see page 246)
Export, Import, and Copy Policies (see page 247)

What is in a User Policy?

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.

Note: For full details about the contents of a user policy, see the *Policy Guide*.

Policy Versions

More information:

Policy Version Numbers (see page 239)
Policy Version Example (see page 239)
Reported and Assigned Policy Versions (see page 241)

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

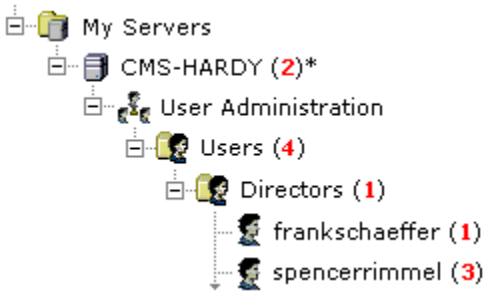
Each value represents the policy version at a specific level in the user or machine tree.

- **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?

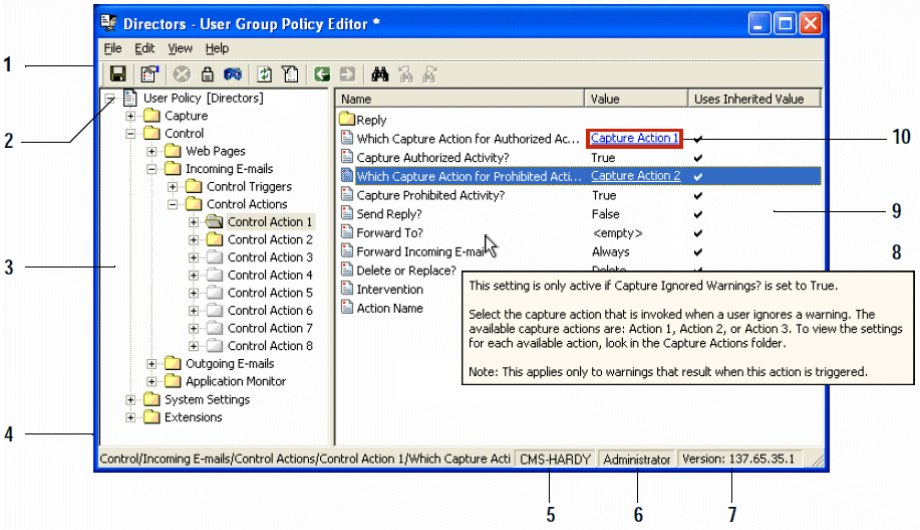
This can happen if an administrator updates a user's policy while the user is not logged on to CA DataMinder. In this situation, the updated (or assigned) policy is held on the CMS but the old policy remains on the client machine. When the user next logs on to CA DataMinder, their client machine reports 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.

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:

Policy Version Numbers (see page 239)
Policy Navigation (see page 165)

Policy Navigation

In the Policy Editor, you can quickly navigate around a policy using hyperlinks and the Back and Forward buttons.

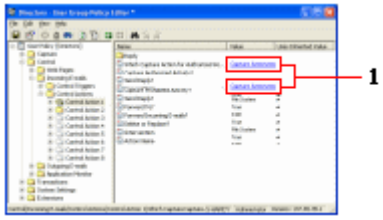
Back and Forward buttons

Use these to jump back to previously selected policy items.

- Click Back to go back to the policy setting or folder that you previously selected.
- Click Forward to return to the policy item you selected before you clicked Back.

Hyperlinks

Some settings are hyperlinked to a dependent setting or folder. For example, each control action has two settings that specify capture actions. Click the hyperlink to jump to the specified capture action.



1 Policy Editor example hyperlinks

Note: These hyperlinked settings are available only in the user policy; there are no equivalent hyperlinks in the machine policy.

Keyboard shortcuts

You can use the arrow keys to navigate through the policy settings. To open a hyperlink, press Ctrl+L.

Note: This keyboard shortcut works only when the setting containing the hyperlink is selected in the right-hand pane.

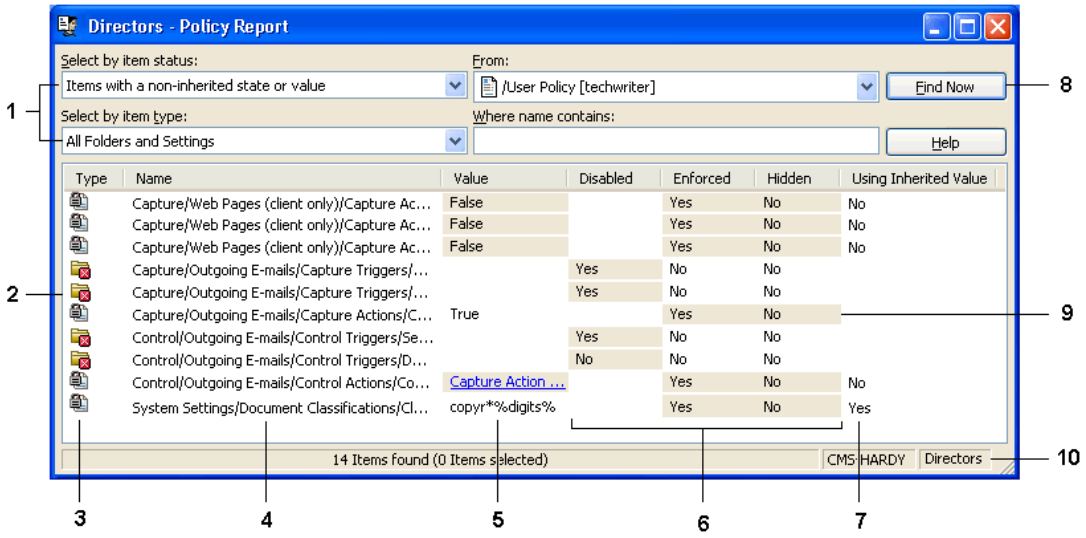
Policy Reports

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.

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.

More information:

Policy Navigation (see page 165)

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 244)

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.

More information:

Policy Navigation (see page 165)

Chapter 14: Troubleshooting

Note: For troubleshooting advice about user policies, see the *Policy Guide*.

This section contains the following topics:

General Troubleshooting (see page 249)
E-mail Troubleshooting (see page 255)

General Troubleshooting

More information:

Can I Rename Users? (see page 250)
Can I Rename CA DataMinder Computers? (see page 252)
Cannot Connect to CMS Because Database Password Has Changed (see page 252)
Clients and Gateways Cannot Connect to CMS (see page 253)
Passwords Are Exposed in the Data Management Console (see page 254)
Data Replication Suddenly Stops When Using ADSL (see page 255)

Can I Rename Users?

You *can* rename users, but the process is complicated and depends on how your CMS policy handles new users.

The first determinant is the *Use Microsoft Windows User Authentication?* policy setting. If CA DataMinder *is* configured to use Microsoft Windows user authentication, verify that any changes to a CA DataMinder user name or its corresponding native Windows user name are closely co-ordinated. If CA DataMinder is *not* configured to use Microsoft Windows user authentication, verify the renamed user is aware that their account name has changed!

The second determinant is the *Account Handling for New Users* policy setting. This controls how the CMS handles new (or unrecognized) users. This setting becomes important if, after renaming a user, you fail to meet the requirements described above.

The relationships between these two policy settings when you rename a user are summarized below:

If *Account Handling for New Users* is set to 'Create New User Account' and:

- *Use Microsoft Windows User Authentication?* is True, see Scenario 1.
- *Use Microsoft Windows User Authentication?* is False, see Scenario 3.

If Account Handling for New Users is set to 'Disable Applications' or 'Ignore' and:

- *Use Microsoft Windows User Authentication?* is True, see Scenario 2.
- *Use Microsoft Windows User Authentication?* is False, see Scenario 4.

Microsoft Windows User Authentication Is Used

If your CA DataMinder installation does use Microsoft Windows user authentication, you must synchronize any name changes for CA DataMinder users with identical changes for the corresponding native Windows users.

This is because CA DataMinder generates and maintains a mapping between each CA DataMinder user account and its corresponding native Windows user account. This means that users do not have to log on to CA DataMinder each time they start up their browser or e-mail application.

If you fail to synchronize these account name changes (that is, you rename one but not the other), the mapping will be broken. To restore this mapping, you must apply the missing name change as soon as possible. Specifically, you must do this before the user next logs on to CA DataMinder (when they start up their browser or e-mail application). If you fail to do so, the consequences depend on how the Account Handling for New Users setting is configured:

- **Scenario 1: 'Create New Account':** CA DataMinder no longer recognizes the user's native Windows credential and so creates a new CA DataMinder user account in the default user group. It is not possible to merge this new user account with the existing account.

- **Scenario 2: 'Disable Applications'** or **'Ignore':** CA DataMinder no longer recognizes the user's native Windows credential and so either waives policy management and allows unrestricted Web and e-mail usage or disables the user's browser and e-mail application.

Ideally, we recommend that you rename the CA DataMinder user account before renaming the native Windows user account. This minimizes the risk of suffering the consequences described above. In practice, the native Windows user name may have changed first, in which case you must rename the CA DataMinder user as soon as possible.

Microsoft Windows User Authentication Is Not Used

If your CA DataMinder installation does not use Microsoft Windows user authentication, CA DataMinder user accounts exist independently of any native Windows user account. This means you can safely rename any CA DataMinder user but you must ensure that the user knows their new account name (and password) before they next log on to CA DataMinder by starting up their browser or e-mail application.

If the user attempts to log on to CA DataMinder using their old credentials (user name and password), then the consequences depend on how the Account Handling for New Users setting is configured:

- **Scenario 3: 'Create new account':** CA DataMinder no longer recognizes the user's old credentials and so creates a new CA DataMinder user account in the default user group. It is not possible to merge this new user account with the existing account.
- **Scenario 4: 'Disable applications'** or **'Ignore':** CA DataMinder no longer recognizes the user's old credentials and so either waives policy management and allows unrestricted Web and e-mail usage or disables the user's browser and e-mail application.

As soon as the user logs on to CA DataMinder using their new user name (and password), their user policy resumes normal operation.

Can I Rename CA DataMinder Computers?

Important! We strongly recommend that you do not rename the CMS or gateway servers. However, you can rename client machines.

CMS and gateways

Renaming the CMS or a gateway can cause severe communication problems between the server and its child machines. This is due to the authentication mechanism used by CA DataMinder machines to ensure data security.

Client machines

You can rename client machines, but be aware that CA DataMinder handles the renamed client as though it were a new machine. That is, the renamed machine is given a new account and inherits the common client policy.

If the local machine policy previously contained customized settings, these will be lost when the client is renamed. You will need to re-configure these settings in the policy for the new machine account.

Cannot Connect to CMS Because Database Password Has Changed

Symptom:

I cannot connect to the CMS because the password for the SQL Server database account has changed. When I attempt to connect to a CMS in the Administration Console, I cannot do so. An error message indicates that 'The logon failed' and the error description reads 'Unable to connect to the database. (Startup Error).'

Reason:

CA DataMinder uses a SQL Server database account to access the CMS database. If your administrators have changed the password for this SQL Server account (typically for security reasons), you must supply CA DataMinder with the new password before you restart the CA DataMinder infrastructure.

Solution:

If you restart the infrastructure before supplying CA DataMinder with the new password, you cannot connect to the CMS. The workaround is to run the following command from the \System subfolder of your CA DataMinder installation folder. This command updates CA DataMinder with the new password:

```
wgninfra -exec wigan/schema/Schema UpdateDBPassword "<DBpassword>"
```

Where <DBpassword> is the new password for the SQL Server database account that CA DataMinder uses to access the CMS database. If the password includes spaces, remember to enclose it in quotes.

To supply CA DataMinder with a new database password

1. Log on to the Administration console as an administrator.
2. Click Tools, Set Database Primary User Password.
3. Enter and confirm the new password.

Clients and Gateways Cannot Connect to CMS

Symptom:

Client machines or gateways fail to connect to the CMS.

Reason:

A change to the CMS system clock can sometimes cause subsequent connection attempts by client machines and gateways to fail. This is because key service objects on the CMS are mistakenly deleted as a result of the unexpected time change.

The problem is very rare, but if it happens the following error message is written to the CA DataMinder system log on the client machine or gateway (you may also see it on-screen):

```
java.rmi.NoSuchObjectException: no such object in table
```

Note: Logfiles are saved in the CA DataMinder \data\log subfolder of the Windows All Users profile.

Solution:

If you suspect that this problem has occurred, or you see this error message, you must restart the CA DataMinder infrastructure on the CMS.

Passwords Are Exposed in the Data Management Console

Symptom:

User policy is configured to obscure passwords submitted to a Web page. But CA DataMinder inadvertently exposes these passwords in the Form Data tab of the Data Management console. In particular, this affects the Hotmail web site.

Reason:

This problem only occurs if a Web page has been designed so that passwords are submitted as hidden data. Normally, when CA DataMinder monitors data submitted to a Web page, it looks in the page's HTML source code for <INPUT type=password> input fields. It then infers that any value entered in this field is a password and must be obscured. But some Web pages submit passwords using other field types, such as <INPUT type=hidden>. CA DataMinder is unable to recognize these passwords and assumes that any information submitted using these input fields is not sensitive and does not need to be obscured.

Solution:

If this problem affects captured data on your CMS, the only solution is to turn off capturing of submitted form data in the user policy.

Data Replication Suddenly Stops When Using ADSL

Symptom:

If a CA DataMinder machine is connected to its parent server using ADSL (Asymmetric Digital Subscriber Line), data replication can suddenly stop because of a lost connection even though ADSL is 'always on'.

Reason:

Under certain network conditions, a broken remote procedure call between CA DataMinder machines can trigger a communication timeout. Because the default timeout can be lengthy (hours, rather than seconds), it can appear as though replication has been permanently lost.

Solution:

If communication resumes between the machines, data replication resumes automatically when the timeout expires. But for usability purposes, you may want to configure a shorter timeout:

1. On both the CA DataMinder machines, go to the CA DataMinder installation.
2. In the \System subfolder locate (or create) the file, JVM.Properties.
3. Add the following line to this file:
   `jvm.define1=sun.rmi.transport.tcp.readTimeout=120000`

   This resets the ADSL timeout to two minutes (that is, 120,000 milliseconds), so eliminating the perception that replication has stopped completely.
4. On both machines, restart the CA DataMinder service.

E-mail Troubleshooting

More information:

CA DataMinder Captures an Email or Attachment With a Virus (see page 256)
Delays When Sending Emails to Many Recipients or Large Distribution Lists (see page 256)
I Cannot Forward Emails That Have Been Redirected (see page 257)
Integration With Outlook Stops Working (see page 258)
Address Lookup Commands Fail if User Display Name is Changed (see page 260)

CA DataMinder Captures an Email or Attachment With a Virus

Symptom:

My organization has suffered a virus attack and the virus scanners failed to prevent it. Infected emails may have been captured and saved in my CA DataMinder database.

Solution:

As part of your cleanup operations after the virus attack, you must also delete any infected emails or attachments from all affected CA DataMinder databases (on the CMS and any gateways or client machines that may also be at risk).

Delays When Sending Emails to Many Recipients or Large Distribution Lists

Symptom:

I experience delays when sending emails to many recipients or large distribution lists.

Reason:

By default, CA DataMinder extracts full details for each recipient from the email server when processing outgoing emails. But if the email is sent to many recipients, or to a very large or heavily nested distribution list, delays can occur while these details are retrieved from the email server. The problem is exacerbated by slow connections between the sender's CA DataMinder machine and the email server.

Solution:

Lower the threshold number of list members that CA DataMinder expands, or set it to extract only basic information from the email for each recipient, or both.

Note: Changing these settings may affect other triggers which include display names or address aliases in, for example, an Included Addresses list.

To edit the user policy

1. Log in to the Administration Console as the primary administrator.
2. Select the "Express Custom Group" in the System Settings folder.
3. Edit the following settings in the user policy.

Maximum Size of Email Distribution Lists

Specify a threshold number of list members. After expanding this number of recipients from a distribution list, or if CA DataMinder detects that expanding a nested distribution list would exceed this number, no further individual recipients are extracted from that list. Details for all extracted recipients are saved as attributes of outgoing emails and can be viewed in the Data Management console. Details of non-extracted recipients are not saved.

Retrieve Full Information for Outgoing Email Recipients?

If you set this setting to False, CA DataMinder only extracts basic information from the email for each recipient. This includes the recipient's display name, email address and the address format. It does not extract a recipient's 'true' display name or email address aliases.

Note: Both the Maximum Size of Email Distribution Lists setting and the MaxNumExpandedRecipient registry value only apply to distribution list members (but not members of personal distribution lists).

I Cannot Forward Emails That Have Been Redirected

Symptom:

In Microsoft Outlook, when an e-mail is redirected, it is included as an attachment in a notification e-mail sent to an alternative account, for example, to a manager. But the manager cannot open the attachment and send the redirected e-mail to someone else because the Send command is disabled in Microsoft Outlook.

Solution:

If the manager wants to forward the redirected e-mail to someone else, the workaround is to:

- Forward the notification e-mail, with the redirected e-mail still included as an attachment.
- Open the attachment and forward the redirected e-mail to its intended recipient (using the Forward command in Microsoft Outlook).

Note: These restrictions do not apply to Lotus Notes. When you forward an email 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.

Integration With Outlook Stops Working

Symptom:

Email triggers stop working for Microsoft Outlook.

Reason:

The Office Safe Mode feature in Microsoft Outlook can disable (sometimes silently) Outlook add-ins that are deemed to prevent Outlook from functioning correctly. This can result in the CA DataMinder Outlook Integration feature (wgnemol.dll) being disabled.

Solution:

Check the Outlook list of disabled items. If the CA DataMinder Outlook Integration feature is listed, try to re-enable the feature. There are two methods for doing this:

Solution 1: Automatically re-enable CA DataMinder Outlook Integration

You must manually add certain values to the following registry key:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA DataMinder\CurrentVersion\EMail
```

Or for 32-bit Outlook client running on a 64-bit OS:

```
HKEY_LOCAL_MACHINE\Software\WOW6432Node\ComputerAssociates\CA
DataMinder\CurrentVersion\EMail
```

Within this registry key, the registry values that you need to add are:

OutlookMonitorIntervalInSeconds

Type: REG_DWORD

Data: Specifies how often CA DataMinder verifies whether the Outlook client agent is disabled in the current session. (A security feature in Outlook can automatically disable certain add-ins). Set this option to 0 to disable monitoring. Specifically, it checks the registry for the wgnemol.dll name and path.

Default: 5 seconds

OutlookRepairDisabledExtension

Type: REG_DWORD

Data: Specifies whether CA DataMinder should re-enable the Outlook client agent if it is found to be disabled. If this registry value is set to a non-zero value and the Outlook client agent is found to be disabled, CA DataMinder re-enables the client agent and writes a Windows application log entry to that effect.

Default: 0 (do not re-enable)

Note: If CA DataMinder discovers that Microsoft Outlook had disabled the Outlook client agent but CA DataMinder has since re-enabled it (for example when Microsoft Outlook is restarted), it writes a Windows application log entry to that effect.

Solution 2: Manually re-enable CA DataMinder Outlook integration

1. On the affected machine, open Microsoft Outlook and choose Help, About Outlook.
2. In the About dialog, click the Disabled Items button.
3. In the Disabled Items dialog, enable the wgnemol.dll add-in (if listed).
4. Restart Microsoft Outlook.

Note: If both methods fail to fix the problem, contact CA Technical Support (http://ca.com/support).

Address Lookup Commands Fail if User Display Name is Changed

(Only applies to Microsoft Outlook 2003 users)

Symptom:

In Outlook 2003, if you change a user's display name in the Active Directory, the new display name does not appear in the Offline Address Book until the next cache update. This may take up to 24 hours.

If the user whose display name has been changed is in a distribution list, the user information in this list will not match the corresponding information in the Offline Address Book until both lists are synchronized at the next cache update. If that distribution list is then the recipient of an e-mail, the fact that its user information differs between the Active Directory and Offline Address Book may result in a trigger not firing.

Solution:

The Microsoft Knowledge Base has an existing workaround, which is also valid for this problem. For further details, see KB831124.

Appendix A: Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are supported by CA DataMinder.

Display

To increase visibility on your computer display, you can adjust the following options:

Font style, color, and size of items

Defines font color, size, and other visual combinations.

The CA DataMinder iConsole also supports a High Visibility mode. This increases the size of text and images in the iConsole screens.

Screen resolution

Defines the pixel count to enlarge objects on the screen.

Cursor width and blink rate

Defines the cursor width or blink rate, which makes the cursor easier to find or minimize its blinking.

Icon size

Defines the size of icons. You can make icons larger for visibility or smaller for increased screen space.

High contrast schemes

Defines color combinations. You can select colors that are easier to see.

Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

Volume

Sets the computer sound up or down.

Text-to-Speech

Sets the computer's hear command options and text read aloud.

Warnings

Defines visual warnings.

Notices

Defines the aural or visual cues when accessibility features are turned on or off.

Schemes

Associates computer sounds with specific system events.

Captions

Displays captions for speech and sounds.

Keyboard

You can make the following keyboard adjustments:

Repeat Rate

Defines how quickly a character repeats when a key is struck.

Tones

Defines tones when pressing certain keys.

Sticky Keys

Defines the modifier key, such as Shift, Ctrl, Alt, or the Windows Logo key, for shortcut key combinations. Sticky keys remain active until another key is pressed.

Mouse

You can use the following options to make your mouse faster and easier to use:

Click Speed

Defines how fast to click the mouse button to make a selection.

Click Lock

Sets the mouse to highlight or drag without holding down the mouse button.

Reverse Action

Sets the reverse function controlled by the left and right mouse keys.

Blink Rate

Defines how fast the cursor blinks or if it blinks at all.

Pointer Options

Let you do the following:

- Hide the pointer while typing
- Show the location of the pointer
- Set the speed that the pointer moves on the screen
- Choose the pointer's size and color for increased visibility
- Move the pointer to a default location in a dialog box

Index

A

Account Import • 37, 230, 231, 235
accounts (new) • 196, 197
address mapping • 189, 190
administration searches • 43, 45, 46
adminstrative privileges • 205
auditing, setup • 101, 108, 109

C

checkpoints • 160, 162

D

diagostics, for machines • 157, 158, 160, 162

E

encryption
    replicated data • 142
    stored data • 143
event auditing, setup • 101, 108, 109
exporting • 247

F

File Scanning Agent (FSA) • 89, 90
free disk space • 138, 139

I

infrastructure • 134, 135

L

log files • 111, 113, 117, 119, 121

M

machine administration • 57, 124, 125, 137, 139, 157
mapping, addresses to users • 189, 190

P

policy roles • 35
privileges • 205
purging events • 147, 148, 149, 150, 151, 152, 153, 154, 155

R

replication • 129, 130, 131, 133
roles, policy • 35

S

security models • 33, 217
suspended machines • 64, 140, 141
Syslog • 121

U

user addresses • 204, 227
user properties • 204, 205, 226, 227

V

version numbers • 239, 241
version numbers, for policies • 239, 241