CA DataMinder

iConsole User Guide

Release 14.6

CA Technologies Product References

This document references the following CA Technologies products:

- CA DataMinder™

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Bulk Edit Duplicate Events (see page 36)—How to create a custom Standard Search that groups duplicate events, and lets you bulk audit child events.

Contents

Chapter 1: About the iConsole

The iConsole is a web-based console that provides searching, reporting, dashboard, and event auditing features.

iConsole users can run reports, search for events, and audit individual events. Users can also create their own customized searches and home pages. Administrators can use the iConsole to manage and test new event searches before making them available to other iConsole users.

This section contains the following topics:

Overview

The CA DataMinder iConsole comprises the following components:

iConsole

The iConsole is a lightweight, browser-based application providing event searching and auditing features. It is primarily aimed at auditors and reviewers.

Front-End Web Server

iConsole users must direct their browser to the front-end web server. That is, they must direct their browsers to a URL based on the name or IP address of the machine hosting the front-end web server.

The front end submits all event searches generated in the iConsole to the application server (see below) and renders the matching events returned from the application server as HTML search results screens. The iConsole screens are generated in Javascript, based on data retrieved using AJAX calls.

Application Server

This component provides the web service that connects to the CMS. It enables all event search and auditing activity conducted in the iConsole to be written to the CMS. It enables iConsole users to search for and retrieve events stored on the CMS and to update audit details for these events.

Keyboard shortcuts

A number of keyboard shortcuts are available. They give you quick access to various tools and links on various iConsole screens. Available keyboard shortcuts include:

Shortcut	Action
Alt+[	Goes to the first page of search results. **Note:** on Firefox use Alt+Shift+[.
Alt+Shift+<	Goes to the previous page of results.
Alt+Shift+>	Goes to the next page of results.
Alt+]	Goes to the last page of results. **Note:** on Firefox use Alt+Shift+].
Alt+/	Highlights the screen element that has focus.

Chapter 2: Logging On

You use the iConsole to search for and audit events stored in a database on the CA DataMinder Central Management Server (CMS). To enable the iConsole to connect to the CMS, you direct your browser to a specific URL (see page 14).

This URL identifies a machine hosting the iConsole server; this server enables communication with the CMS and also generates the iConsole screens displayed in your browser. Typically, browsing to this URL takes you directly to the iConsole home page. However, depending on how CA DataMinder is configured, you may first need to log on (see page 15) to the CMS.

Likewise, if your browser is in a different domain to the iConsole server, a Windows dialog first prompts you for a user name and password before you can connect to the target domain (see page 16).

This section describes how to start up the iConsole and what information you must supply when you log in. It also summarizes how the iConsole connects to your CMS.

This section contains the following topics:

Start Up the iConsole

You use the iConsole to search for and review captured e-mails, files, web pages and IM conversations.

In Internet Explorer, browse to the iConsole URL, typically provided by your administrators. This URL takes the following format:

`http://FE_Server/Virtual_Dir`

FE_Server

The name or IP address of the machine hosting the iConsole server.

Virtual_Dir

The name of the virtual directory for the iConsole server.

Default: 'cadlp'.

Note: Your administrators may have renamed the default to suit your organization.

Example: If your iConsole server is hosted on the machine UX-WebSvr-01, enter the following iConsole URL in the browser address box:

`http://UX-WebSvr-01/cadlp`

The next page or dialog that you see depends on how CA DataMinder is configured on your network. See the next section for details.

Which Screen is Next?

After you browse to the iConsole URL, the next screen or dialog that you see depends on how CA DataMinder is configured on your network:

iConsole Home Page

Most users are taken directly to the iConsole home page after browsing to the iConsole URL.

iConsole Review Page

If the iConsole home page has been deactivated, users start on the Review page by default.

Users with appropriate privileges, such as reviewers, can run searches and reports.

iConsole Logon Page

Typically, the iConsole uses your Windows logon credentials to authenticate you on the CMS. Consequently, users are taken directly to the iConsole home page or Review page without needing to log on. Only if the CMS cannot authenticate you, the iConsole logon page appears.

Windows 'Connect to <domain>' Dialog

If your browser is not in the same domain as the iConsole server, the Connect to Domain dialog appears.

iConsole Logon Page

When you browse to the iConsole URL, you may be taken first to the iConsole Logon page. This happens if the CMS cannot authenticate you. You must now supply your CA DataMinder credentials to go to the iConsole home page:

CMS

Select a CMS from those available. By default, the iConsole server only supports a single CMS; it must be manually configured to support multiple CMSs.

Username

Enter your CA DataMinder user name.

Password

Enter the password for your CA DataMinder user account.

Connect to Domain Dialog

When you browse to the iConsole URL, the Windows 'Connect to <domain>' dialog may appear. This happens if your browser host machine is not in the same domain as the iConsole. You must authenticate yourself to the iConsole server domain before you can go to the logon page (see page 15).

When this dialog appears, you must supply the user name and password of a Windows account that is recognized by the iConsole server domain.

Logon FAQ

Why must I log on?

If the CMS cannot authenticate you, you are taken to the iConsole Logon page . This happens if:

- Your CMS or CA DataMinder account is not set up for Single Sign-On (see page 171), or
- Your CMS or CA DataMinder account is set up for Single Sign-On, but you are accessing the iConsole from outside the CMS network domain.

Can I change my password?

If you are required to enter a password when logging on to the iConsole, a user with administrator privileges can change that password:

1. Click Settings on any iConsole page.

   The Preferences screen opens.

2. Click 'Change Password'. You need administrator privileges to see this button.

   The Change Password screen opens.

3. Type in your current password, then type in and confirm your new password, and click Apply.

   Your password is changed.

If my iConsole session times out, must I log on again?

By default, iConsole sessions terminate automatically if no user activity (key presses or mouse clicks) is detected for 20 minutes. If this happens, you are taken to the iConsole Logon page (see page 15). This automatic session timeout is for security and performance reasons.

If your iConsole session times out and Single Sign-on is enabled, you can click Connect or press Enter without re-entering your user name and password. If Single Sign-on (see page 171) is not enabled, you do need to re-enter your user name and password.

Can I change the iConsole session timeout?

Yes. The session timeout is configurable. To lengthen or shorten the timeout, your iConsole administrators must modify a registry value on the iConsole server. Contact your iConsole administrators for further details.

Can I log on as different users in Internet Explorer 7 or later?

No. It is not possible to use Internet Explorer tabs to log in as different users because of the following limitation in Microsoft Internet Explorer 7 and 8:

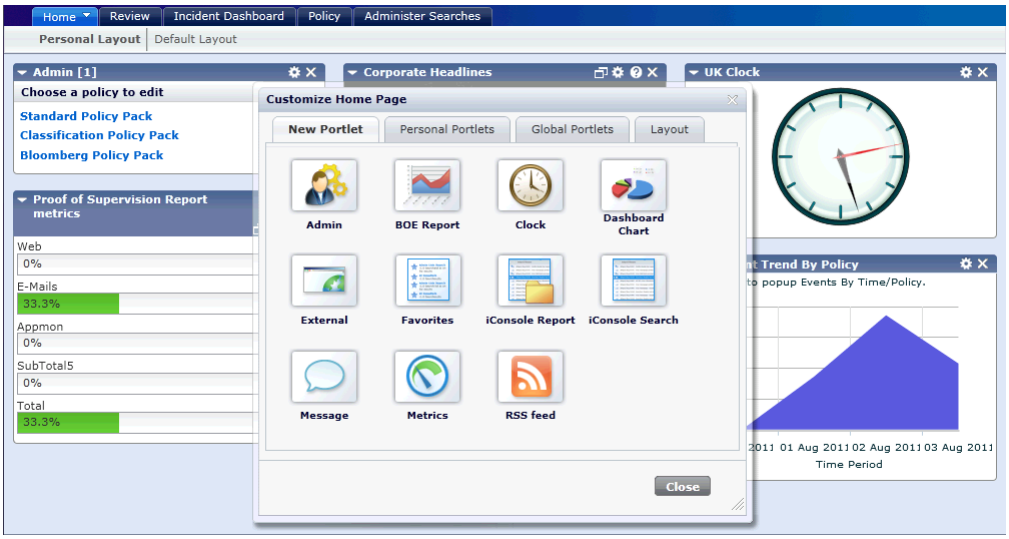
Internet Explorer enables you to view multiple web sites in a single browser window using tabs. In the iConsole, if a user tries to log in as different users in two of these tabs, then the session login details of the iConsole in the first tab is overwritten. This is because IE7 tabs share session cookies and so tabs must share the session for a particular domain or URL.

Chapter 3: Home Page

This section contains the following topics:

About the Home Page

The home page is displayed every time you log on to the iConsole. You see a default home page if the administrator has defined one. You can choose what information is included on the home page, for example, shortcuts to favorite searches, dashboard charts, reports, and reminder messages. You can activate or deactivate the personal home page by configuring your personal settings.



About Portlets

Portlets are elements on the home page that display relevant information, for example reports, charts, or lists of searches.

All Portlets

Users can add portlets to their home page and customize these portlets to display the information that they use most often.

Users can collapse or move portlets to declutter their home page. They can also open portlets in a new window. For example, if they have an 'External' portlet on their home page that links to a favorite web site, they may prefer to view this portlet in a new window.

Personal Portlets

A *personal portlet* is shown on the home page of the user who created it. By default, personal portlets are not available to other users.

Note: A user can only create personal portlets if their user role has the 'Allow Portlet Creation' setting.

Global Portlets

A *global portlet* can be included on the home page of any user.

Administrators can designate a new portlet as a global portlet by selecting the ‘Anyone can use this portlet’ checkbox when you specify the new portlet's parameters.

Note: Only administrators with the 'Admin: Manage iConsole' privilege can create global portlets.

Mandatory ('Pinned') Portlets

A mandatory portlet does not have a Close button and users cannot remove it from their home page.

Administrators can designate a global portlet as mandatory by 'pinning' the portlet to every home page.

Note: Only administrators with the 'Admin: Manage iConsole' privilege can create mandatory portlets.

More information

Create a Personal Portlet (see page 28)
Create a Global Portlet (see page 143)

Chapter 4: Personalizing the iConsole

Typically, ordinary users are permitted to personalize the iConsole. For example, they can create a custom home page that displays when they log in and which contains the portlets they need. They can also specify and save their own custom versions of the standard searches and reports.

Note: Administrators with the 'Admin: Manage iConsole' privilege control how far ordinary users can personalize the iConsole. For example, an organization may allow managers considerable freedom to personalize the iConsole but lock down the iConsole when reviewers log on. See the 'iConsole Administration' section for details.

This section contains the following topics:

More information:

iConsole Administration (see page 141)

Configure Personal Settings

You can configure personal settings for the iConsole. For example, you can configure auditing behavior and how search results are displayed.

To configure your personal iConsole settings

1. Click the Settings link in the top right of the iConsole screen.

   The Settings dialog appears.

2. Configure personal settings as required. Available settings are shown on the following tabs:

   - General (see page 148)

     These settings configure the default behavior for iConsole home pages.

   - Search (see page 24)

     These settings control how search results are displayed.

   - Printing (see page 23)

     These settings determine whether printed search results include the event text content, summary details, and extended information.

   - Audit (see page 23)

     These settings control audit behavior in the Search Results screen.

   - BusinessObjects (see page 25)

     These settings control which BusinessObjects features are available in the iConsole. For example, you can choose whether to show BusinessObjects reports in the Review tab. You can also specify the report format (HTML or PDF) and the folder where the reports are saved in InfoView.

3. (Optional) Click Change Password to reset your CA DataMinder password. You must enter this password when you log onto any CA DataMinder console.

   Note: The Change Password button does not appear if you use Single-Sign On.

4. Click the OK button.

   Your personal settings are active.

More information:

Audit Settings (see page 23)
Printing Settings (see page 23)
Search Settings (see page 24)
General Settings (see page 24)
BusinessObjects Settings (see page 25)

Audit Settings

These settings control audit behavior in the Search Results screen.

Move to Next Event After Auditing

Specifies whether focus moves automatically to the next event after an event has been reviewed or audited.

Remove Events After Auditing

Specifies an event is removed from the Search Results after it has been reviewed or audited.

Scroll Past Headers in Email Pane

Specifies whether the display scrolls automatically past the recipient and subject details to the body text when reviewing an individual email event.

Show Incidents / Show Issues / Show Event History

Specifies whether incident details, audit issues and the event history are displayed in the right-hand pane when reviewing an individual event.

Note: CA DataMinder generates an *incident* each time a policy trigger fires.

Incidents Display / Issues Display / Event History Display

(Applicable only if the corresponding 'Show' check box is selected.) Specifies the initial level of shown in the right-hand pane when reviewing an individual

Printing Settings

These settings determine whether printed search results include the event text content, summary details, and extended information.

Print Content

Prints the text content of captured events (if available).

Print Event Summary

Prints the event metadata. This includes details about any triggers that fired plus an indication of why they fired.

The metadata also includes details such as the event type, participants, timestamp, and event source.

Print Audit Summary

Prints any audit details associated with the event, including audit histories for individual audit issues.

Search Settings

These settings control how search results are displayed.

Search Results Page Size

Specify the maximum number of results per page.

Multi-line Row

Specify whether details for individual events can wrap over multiple lines of text.

Show results in bold until viewed

Specify whether events are shown in bold in the results screen if you have not viewed them yet. After you view an event, it is shown in normal text.

Content Server

If your iConsole supports content searches, you can specify which content proxy server to use.

The content proxy server links the console to a content database. You may prefer to manually select a content proxy server you have:

- Multiple proxy servers connected to different content databases. Choose the proxy server that is connected to the database containing the captured data you want.
- Multiple proxy servers connected to a single content database. Choose the proxy server with, for example, the fastest or the most secure database connection.

General Settings

These settings configure the default behavior for iConsole home pages.

High Visibility

Specifies whether you want to display the home page with a larger, more easily readable font.

Show Home Page

Specifies whether a home page is displayed when you log into the iConsole.

Remote Access

(Applies only if you connect to the iConsole using Remote Desktop Connection)

Optimizes the iConsole display for RDC connections. In particular, this setting turns off graphics features such as background animations in iConsole dialogs. Such graphics can affect iConsole performance during RDC sessions.

BusinessObjects Settings

These settings control which BusinessObjects features are available in the iConsole. For example, you can choose whether to show BusinessObjects reports in the Review tab. You can also specify the report format (HTML or PDF) and the folder where the reports are saved in InfoView.

Use BOE Integration

Allows you to run BusinessObjects reports for CA DataMinder.

Default Format for BOE Reports

Specifies the output format for CA DataMinder BusinessObjects reports. The supported formats are PDF and HTML.

Allow BOE Portlets

Allows you to add BusinessObject report portlets to your home page.

Allow BOE Reports

Adds BusinessObjects reports for CA DataMinder to the BusinessObjects page of the iConsole Review tab.

Show a Link to InfoView

Adds an InfoView link to the BusinessObjects page of the iConsole Review tab.

Show Personal Reports

Adds your customized BusinessObjects reports to the BusinessObjects page of the iConsole Review tab.

Personal Reports Folder

Specifies the folder where your customized BusinessObjects reports for CA DataMinder are found.

Your customized BusinessObjects reports for CA DataMinder are available in InfoView on the Document List page. Specify the folder on the Document List page that contains your customized BusinessObjects reports.

Customize Your Personal Home Page

You can customize your home page to display information that you most commonly need.

If the administrator has configured a default home page, it is displayed the first time that you visit the Home tab. If there is no default home page, the welcome message instructs you how to create a personal home page.

Note: If you see no Home tab, you can activate the home page in your personal Settings. Contact your administrator if this feature is deactivated globally.

To customize your personal home page

1. Click the Home tab.
2. Click the  Customize link in the top right of the iConsole screen.

   The Customize Home Page dialog displays.

3. Specify the portlets and layout for your home page:
   - New Portlet tab

     (Available only you have the 'Allow portlet creation' permission) Use this tab to create new portlets for your home page.
   - Personal Portlets tab

     Use this tab to manage the personal portlets on your home page. You can add, remove, rename, or delete these portlets.
   - Global Portlets tab

     Use this tab to manage the global portlets on your home page. *Global portlets* are predefined portlets that have been assigned to your user role.
   - Layout tab

     Use this tab to manage the layout of your home page. The layout defines the columns and portlets included on a home page.
4. Click Close.

   The home page is displayed with the selected layout.

To arrange the home page

1. Drag portlets and drop them into their desired location in a column.
2. (Optional) Click the  Settings link in a portlet titlebar to configure the portlet.
3. (Optional) Click Collapse Portlet in the titlebar of a portlet to reduce clutter on the screen.

   The home page layout is saved automatically.

Note: You can also Create a personal portlet (see page 28) and add it to your home page. This option is only available if you have the 'Allow portlet creation' permission.

Create a Personal Portlet

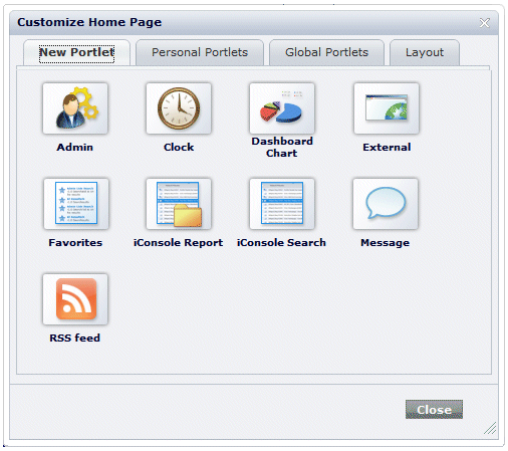
You can create personal portlets for your home page. A personal portlet only appears on your home page unless you choose to share the portlet with other users.

Note: Contact your administrator if this feature is not available to you.

To create a personal portlet

1. Click the Home tab.
2. Click the Customize link in the top right of the iConsole screen.

   The Customize Home Page dialog displays.

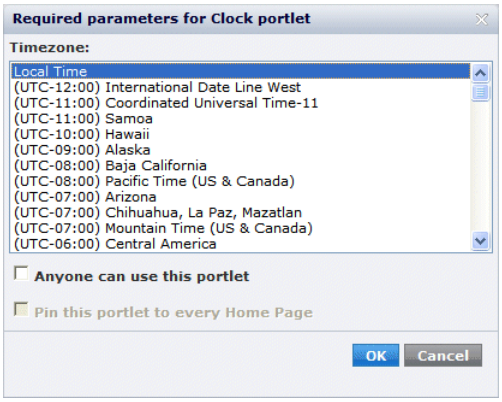


Customize Home Page dialog, New Portlet tab

3. Click the type of portlet that you want in the New Portlet tab.

   The Required Parameters dialog appears.

4. Specify the portlet details.



Example Required Parameters dialog

5. (Optional) Uncheck the 'Anyone can use this portlet' check box.

   This creates a personal portlet that only appears on your home page.

6. Click OK to return to the Customize Home Page dialog.
7. (Optional) Change the portlet title.
   a. Go to the Personal Portlets tab.
   b. Click the Actions button for the portlet you created.
   c. Click Rename and enter the new title. You can also add a brief description.
   d. Click OK to return to the Customize Home Page dialog.
8. Close the Customize Home Page dialog.

   The portlet displays on your home page with default settings. You must now edit the portlet settings.

More information:

Edit a Portlet (see page 29)

Edit a Portlet

Use the Home Page Portlet Wizard to edit portlet settings.

Note: Click the question mark in the portlet title bar to get details about the portlet.

To edit a portlet

1. Click  Settings in the portlet title bar.
2. Click the  Portlet Definition button to launch the Home Page Portlet Wizard.
3. Specify the portlet settings.
4. Click Finish to close the wizard.

Chapter 5: Searching for Events

This section contains the following topics:

Available Searches

The following standard searches are available:

Content Search

Retrieves events based on their text content. Content searches can identify clusters of related documents, defined by their characteristic text patterns that reveal a shared subject or theme.

Content searches use intelligent pattern-matching technology to analyze the text content of indexed events in a content database and retrieve events that match the search criteria.

Note: Content searches are only available if explicitly included in your license agreement.

Data At Rest Standard Search

Retrieves Data At Rest events that match specific criteria. These events typically include files and other items scanned by the File Scanning Agent (FSA) and Client File System Agent (CFSA), plus files stored in an archive.

Data In Motion Standard Search

Retrieves Data In Motion events that match specific criteria. These events include: emails; network events entering or leaving your corporate network, including webmail and IM attachments and FTP file transfers; IM conversations captured by CA DataMinder Network; and web events, including file uploads.

Data In Use Standard Search

Retrieves Data In Use events that match specific criteria. These events include: files copied or saved to removable devices (such as USB flash drives), writable CD and DVD drives, and network locations; files sent to a printer; and instances when a user runs a specific application.

Quarantine Search

Retrieves quarantined emails.

Reviewer Search

(Available only with the Review Queue) Retrieves events in a user's personal review queue. These are events waiting to be reviewed.

Recent Incidents

Retrieves all events for a specified date range.

Standard Search

Retrieves events that match specific criteria. It covers all event types and includes all the commonly used search filters. This search include Settings to bulk audit duplicate events (see page 36).

More information:

Bulk Audit Duplicate Events (see page 36)

Run a Search

The iConsole Review tab lists the available searches.

To run a search

1. Go to the Review tab.
2. Click the Searches link.

   The Searches page lists the available searches. Icons identify the search type:

   Standard searches are available to all users logged on to the CMS.

   Customized searches are your own saved and customized searches. They are not available to other users.

   Derived searches are customized searches available to all users.
3. Click the search you want to run.

   Events matching the search parameters are shown in the Search Results screen.
4. (Optional) Click Add to Favorites ( ) to bookmark a commonly used search in your web browser. Open the bookmark to run this search directly.

Customize a Search

You can customize an existing search. For example, you can change the default date range. When you customize a search, it is added only to your searches list. It is not available to other users.

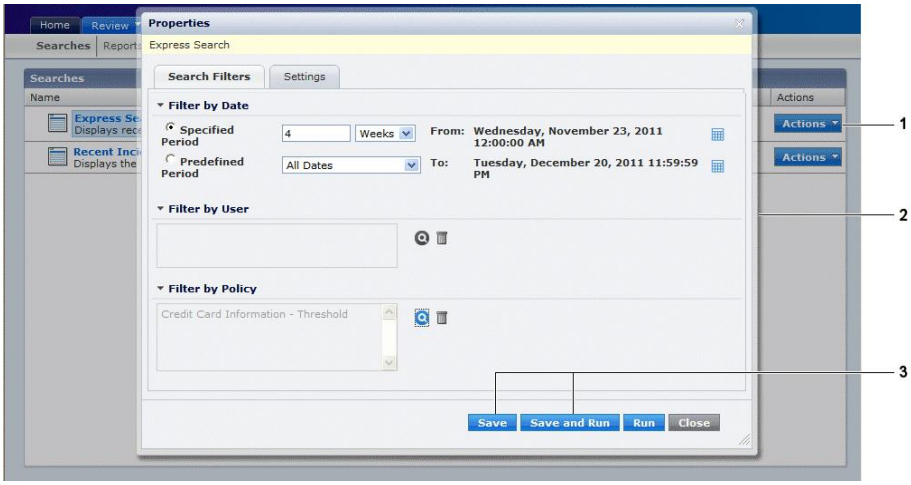
To customize an existing search

1. Go to the Review tab.
2. Click the Searches tab.

   The Searches page lists the available searches.
3. Click the Actions button (**1** in the screenshot below)

4. Click Edit Properties to customize a search.

   The Search Properties screen displays (**2**). Settings are grouped into tabs, such as Search For and Event Attributes.

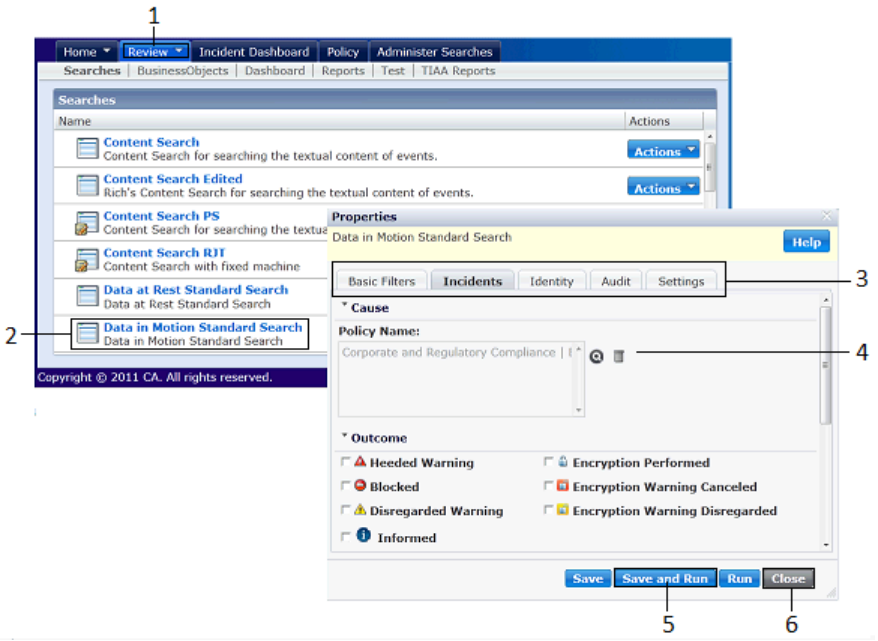


5. Edit the search properties as required.
6. Click the Save or Save and Run buttons (**3**) to save your changes.
7. Enter a name and description for the customized search.

   Your new customized search is added to your Searches list.
8. Click the Action button (**1**) to rename or delete customized searches.

About the Search Properties Page

This screen shows the search properties that you can edit to customize your search.



Example search properties page

1. **Review tab.** Lists the available searches, reports and dashboards.
2. **Search list.** Shows the search you are currently editing.
3. **Filter tabs.** Related search properties are grouped into tabs.
4. **Search filters.** Edit as required to customize your search.

   For some text fields, you use a Search and Select button and a Clear button to specify the filter. You do not type the items directly into the text field.

   - Click Search and Select to open a Selector dialog, where you can choose the items you want.
   - Click Clear to empty the text box.
5. **Save and Run buttons:** You can save your changes as a customized search.
6. **Close button:** Click to hide the search properties page and return to the Review tab.

More information:

Search Results screen (see page 48)

Useful Customizations

The following sections describe some of the most common search customizations, including how to specify date ranges and how to target events associated with specific users or groups.

More information:

Bulk Audit Duplicate Events

Often, the same events are ingested into the CMS from multiple Policy Engines, and are displayed as multiple duplicate rows in the iConsole. You can customize a standard search to list duplicate events with specific criteria, and group these duplicates together.

A de-duplication search saves you the effort of identifying and handling duplicate events. You create and run your custom search, select a parent event, and apply audit actions (including print, review, escalate) to its child events in bulk.

Follow these steps:

1. Go to the Review tab and click the Searches link.

   The Searches page lists the available searches.

2. Click the Actions button on the Standard Search.

3. Click Edit Properties create a customized Standard Search.

   The Search Properties screen displays.

4. Open the Settings tab.
5. Specify Rollup Key search criteria by selecting *one or a combination* of the following Available Items:

   Time Stamp

   Lists similar events with the same time stamp as duplicates.

   Subject

   Lists similar events with the same subject as duplicates.

   Users

   Lists similar events with the same user as duplicates.

   Policy ID

   Lists similar events with the same Policy ID as duplicates.

   Pre-Defined (From Database)

   Lists events that match on EventTimeStamp +/- 30 sec, subject, sender, and trigger count. This pre-defined search requires you to create a custom scheduled task to identify duplicate groups of events, and to insert those groups of records into the Wgn3RelatedEvent table.
6. (Optional) Specify other search criteria for your standard search.
7. Click Save, and enter a name and description.

   Your custom de-duplication search is added to your Searches list.

More information:

Available Searches (see page 31)

Incoming or Outgoing E-mails

You can search for incoming or outgoing e-mails or IM comments associated with specific e-mail addresses.

To search for incoming or outgoing e-mails

1. Go to the Basic Filters tab of the Search Properties screen.
2. Select the Filter By Type option.
3. In the E-mail Events or IM Events sections, edit the **Addressee1**, **Direction** and **Addressee2** fields to specify incoming or outgoing events.

Examples

These are based on two users, Frank Schaeffer, whose e-mail address is fschaeffer@unipraxis.com, and Lynda Steel, whose address is lsteel@unipraxis.com.

- **E-mails sent from Frank to Lynda:** To only search for e-mails sent from Frank to Lynda, set the Address and direction fields to:

  Addressee1: fschaeffer

  Direction: 'Addressee1 sent e-mails to Addressee2'

  Addressee2: lsteel

- **E-mails sent in either direction:** To search for all e-mails sent between Frank and Lynda, set these fields to:

  Addressee1: fschaeffer

  Direction: 'Addressee1 shared e-mails with Addressee2'

  Addressee2: lsteel

- **All e-mails sent by Frank:** To search for all e-mails sent by Frank to anyone, set these fields to:

  Addressee1: fschaeffer

  Direction: 'Addressee1 sent e-mails to Addressee2'

  Addressee2: <blank>

- **All e-mails received by Frank:** To search for all e-mails received by Frank (sent from anyone), set these fields to:

  Addressee1: fschaeffer

  Direction: 'Addressee1 received e-mails from Addressee2'

  Addressee2: <blank>

Note: An automatic *** wildcard** is appended automatically to any entry in the From and To fields. As a shortcut, you need only type 'fschaeffer' to match fschaeffer@unipraxis.com and 'frank' to match frank.schaeffer@unipraxis.com. The examples below use these automatic wildcards instead of the full e-mail addresses.

Internal Events

You can explicitly search for internal e-mails, Web pages, or IM conversations. CA DataMinder flags events as internal when:

- **Outgoing e-mails:** All the recipient addresses match an internal address pattern (for example, *@unipraxis.com).
- **Incoming e-mails:** The sender's address matches an internal address pattern.
- **IM conversations:** All participants have an e-mail address that matches an internal address pattern.
- **Web events:** The Web site address matches that of an intranet URL.
- **Network events:** Internal network events are files and attachments captured by an NBA located on the boundary of two internal subnets. Processing of internal network events is not currently supported, but may be introduced in future releases.

Note: Internal address patterns and intranet URLs are defined in the user policy. For details, see the Administration console online help; search for 'internal e-mails' or 'intranet addresses'.

To search for internal or external events

1. Go to the Basic Filters tab of the search Properties screen.
2. Select the Filter By Type option.
3. In the E-mail Events or IM Events sections, choose the option you want from the Type field. For example, choose Internal Only.

File Events: Name, Host or Path

You can search for files on a specific host machine or files with a specific name or path.

To search by file host, path, or name

1. Go to the Basic Filters tab of the search Properties screen.
2. Select the Filter By Type option.
3. In the File Events sections, edit the Host, Path and Name fields to specify the host (machine name), path to the file, or file name.

Title or Subject

For e-mails, you can search by subject text; for IM events, you can search by the conversation title.

To search by title or subject

1. Go to the Basic Filters tab of the search Properties screen.
2. Select the Filter By Type option.
3. In the E-mail Events or IM Events sections, edit the Subject field.

   If the subject contains % * _ ? characters, you must prefix them with a \ backslash. For example, to search for e-mails with the subject '25% stock rise!' you enter:

   25\% stock rise

Blockings or Warnings

You can search for events associated with particular control actions. For example, you can search for e-mails that triggered a warning or were blocked.

To search by control action

1. Go to the Incidents tab of the search Properties screen.
2. Select the Selected Triggers option.
3. Choose the event types that you want, such as Blocked or Disregarded Warning.

Smart Tags, Classifiers and Triggers

You can also search for events captured by specific triggers or events captured when CA DataMinder detected a match with particular document classifiers or smart tags.

To search by smart tags, classifiers, or triggers

1. Go to the Incidents tab of the search Properties screen.
2. Edit the Trigger Name, Smart Tag, Smart Tag Value or Classifier Name fields.

   Type the name directly or click the Search and Select button to display a dialog that lists all the available items.

Policy Classes

You can also search for events by a specific class of policy trigger or category.

To search by policy class

1. Go to the Incidents tab of the search Properties screen.
2. Edit the Policy Name field to select the policies or policy classes.

   Click the Search and Select button to display a dialog that lists all the available items.

Severity Scores

You can search for captured events based on their severity scores. By default, the severity bands are: Not Set, Low, Medium or High.

To search by severity

1. Go to the Incidents tab of the search Properties screen.
2. Click the severity level.

   Note: To view the severity of each event in the Search Results screen, you must add Severity to the list of visible columns. By default, this is a hidden column.

Users or Groups

You can search for captured events associated with specific senders, recipients, or user groups.

To search by user or group

1. Go to the Identity tab of the search Properties screen.
2. Specify the following fields:

   Select

   Click User or Group.

   Name Match

   Type the name of the user or group you want to search for.

   The iConsole adds leading and trailing * wildcards automatically when you enter a name (or name fragment).

   If searching by user name, be aware of domain prefix and case-sensitivity requirements.

   Specific Match

   Click Search and Select to search for users or groups. Click Clear to empty the text box.

   The Selector dialog allows you to search for users and groups by name and add the ones you want to your event search.

Audit State

You can search for events by audit state. For example, you can refine the search to focus on events with specific audit attributes or with issues raised by a particular auditor.

To search by audit state

1. Go to the Audit tab of the Search Properties screen.
2. Select the following check boxes as necessary:
   - **Unreviewed Events:** These events may have been viewed by an auditor, but no issue was raised.
   - **Reviewed Events:** These events have one or more issues raised against them.
   - **Bulk Reviewed Events Only:** These events have been audited in bulk. Individual events may not have been viewed by an auditor.
3. Select the Field 1, 2 and 3 attributes as necessary.

   For example, you can search for events with a specific audit status, or events with no audit status at all.
4. If required, enter the name of a particular auditor to retrieve events with issues raised by a particular auditor.
5. If required, enter a specific comment (or comment fragment) to retrieve associated events.

Date Ranges

When searching for events captured over a specific period, you can specify the start and end dates, and even the start and end times on those days. For the predefined iConsole searches:

To search by date

1. Go to the Event Date Range tab of the search Properties screen.
2. Set the date range for your search.

   You can configure the iConsole to only display results for a specific period.

   Specified Period

   Choose the search period. For example, you can search for events captured within the last 7 Days, or between two specific dates. Click the Show Calendar button to choose a specific date.

   Predefined Period

   Choose from the list of available time periods. For example, you configure the search or report to include all results for This Calendar Quarter.

Fingerprinted Files

You can use the iConsole to search for fingerprinted files detected by CA DataMinder. You need to filter your searches either by trigger name, (specifying the content agent triggers that detected the files) or by policy class (specifying the class assigned to these triggers).

To search for fingerprinted files

1. In the iConsole, edit the properties of the search that you want to run.
2. Go to the Incidents tab of the Search Properties screen.
3. Do one of the following:
   - In the Trigger Name field, choose the relevant trigger.
   - In the Policy Name field, choose the policy class associated with the relevant content agent.
   - **Note:** Only the standard CA DataMinder searches enable you to filter your search by trigger name or policy class.

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.

View Search Results

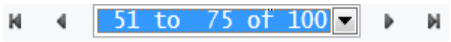
When using the iConsole to review events, you can update the audit status for events and individual event issues.

To view the search results

1. Run a search in the iConsole.

   The search results screen lists all events matching the search criteria.

2. Use the navigation buttons to browse the search results.

3. (Optional) You can review multiple events at the same time. For example, you may want to set the audit status for a several events to 'Approved'. Use the audit buttons for bulk auditing of multiple events:

   These buttons are configured in the Administration console. They allow you to instantly audit events in the iConsole, changing specific audit details from one value to another.

4. (Optional). Zero in on individual events. Click any event to view its details at the bottom of the page.
5. You may be prompted to enable automatic auditing. If you have the appropriate privilege, the Audit Operations dialog appears when you first review an event. This dialog asks whether you want to update the event's history each time you view an event.
6. View details for the current event.

   The search results screen shows the event details in three panes:

   Content pane

   Shows the unformatted text content (if captured).

   Information pane

   Shows key event details such as its severity, plus a summary of any policy applied to the event.

   Audit pane

   Shows any issues raised against the event, plus the event's history (such as changes to its audit status).

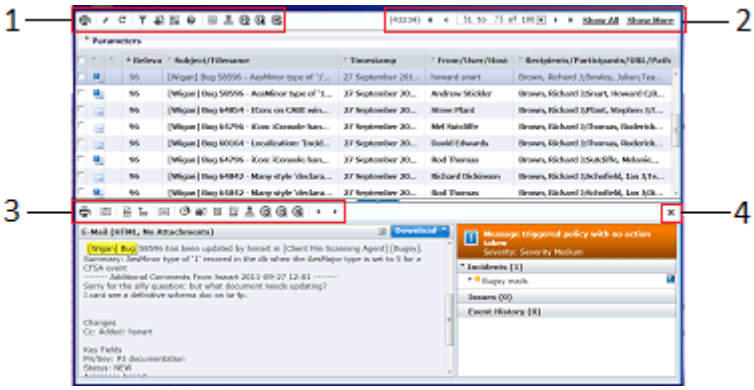
   Note: Hold down the keyboard Ctrl button and click the Content, Information or Audit toolbar buttons to hide or show individual panes.
7. (Optional) While viewing an event, you can do any of the following:
   - Change the view. For example, you can choose a print-friendly view.
   - Download the event (if full details were captured). Find the Download button in the content pane.
   - Update the event issues. Click the New Issue button  to add a new issue.
   - Change the expiry date. Click the Expiry Date button  to change when the event becomes eligible for purging from the CMS database
   - Release or reject quarantined events.

More information

Search Results screen (see page 48)
Filter the Search Results (see page 49)
View an Event in Context (see page 50)
Save an event as a link (see page 50)
Display a User's Account History (see page 51)
Download an Event (see page 52)
Print an Event (see page 53)

Search Results screen

This screen lists events matching your search criteria. Use this screen to review or audit events.



Example search results page

1. **Results toolbar.** Use these buttons to, for example, edit the search properties, filter the search results by key text, download results, and choose which columns to display.

   Use the audit buttons and the Expiry Date button to update audit details for multiple events simultaneously.

2. **Result navigation controls:** Use these buttons to browse the results pages.
3. **Event toolbar:** When you click an individual search result, this toolbar displays. Use these buttons to, for example:
   - Display the Content, Information and Audit event tabs.
   - View the event in context. That is, view the events captured immediately before and after the current event.
   - Audit the event. For example, you can create a new issue, approve the event, or change its expiry date.
4. **Close button:** Click to hide the event panes and return to the results list.

Filter the Search Results

When reviewing events, you can use the Filter Results button to only display particular events.

Search filtering matches text in all visible results columns. For example, if you filter events on the word ‘red’, then only events with ‘red’ in one of its columns (this includes, for example, ‘Fred’), appear in the filtered list.

To filter your search results

1. In the search results screen, select the Filter Results button.

   Note: The Filter Results button is not available when viewing events in Excel View, or when a search returns only one event.

2. Enter the filter text. These are the keywords that you want to use to filter the search results.

   For example, type 'escalate' to filter your search results to only include events with an audit status of Escalate.

   Note: If other events contain the word 'escalate' in a different field on the search results screen (for example, the Subject field), then they will also appear in the filtered list.

3. Click Apply.

   The results list shows only those events containing the specified keywords.

4. If you filter the results again, the iConsole filters on **all** search results and not just the results of the previous filter.

View an Event in Context

When viewing search results, you can zero in on an individual event to view the events captured immediately before and after it. This can be useful if, for example, you want to trace the activity of an individual user over a particular period or if you want to follow the trail of Web activity that culminated in a warning or blocking.

You view an event's context in a specific Search Results screen. This screen highlights the current event and shows events for the same user captured immediately before and afterwards.

To view an event in context

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click the Context button  .

   A separate Search Results screen appears displaying events that were captured before and after the selected event.

Save an event as a link

Event links allow you to quickly and easily access an event. They also allow you to save events that include unusual or unexpected information. When you save an event as a link, a shortcut to that event is added to your Favorites in your browser.

To save an event link

You can save event links in the search results screen.

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click the Save Event as Link  button and enter a name for the event shortcut

   A shortcut to the event is added to your Favorites.

   Note: Normally, when you click the event shortcut in Favorites, the iConsole takes you directly to the event page. But if Single Sign-on is not enabled, it takes you instead to the Logon page.

Display a User's Account History

After you run a search, you can view account details for any CA DataMinder user listed in the search results, including the user history and group history.

The user history shows the date and details of any name changes for the current user, for example, if the user has married. The group history shows when a user was moved from one group to another.

To display a user's account history

In the Search Results screen, click a user name in the From/User/Host column.

The User Details dialog shows the selected user's name, e-mail addresses, user history, and group history

Download an Event

When viewing search results, you can download individual events from the CMS. This is useful if a colleague needs to view an event but does not have access to the iConsole. Various download formats are supported.

To download an event

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click the Download button and choose the format for the downloaded events:

   Microsoft Outlook Message

   (Available for emails only) Choose this format if you want to view an email as the recipient or sender saw it, with its original formatting. The email is downloaded from the CMS as an .msg file. You can then open this file in Microsoft Outlook.

   Note: Some email types cannot be downloaded in their original format. These include emails imported from EVF files or captured via a Domino Server. You can download such email types as, zip, text, or XML files.

   ZIP Archive

   Downloads a compressed version of the event. For emails and IM conversations, the zip file contains an RTF representation of the email or conversation plus any attachments.For files, the zip file contains an RTF representation of the file content plus the file itself.

   Text File

   Downloads a text file containing the event metadata and text content. For emails, the text file contains the email property details (such as sender and recipient information, details about attachments, plus the body text. For IM conversations, the text file contains participant information plus the conversation comments.

   Metadata XML

   Downloads an XML file containing the event metadata only.

Print an Event

When viewing search results, you can print multiple or individual events.

To print an individual event

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click the Printable View button in the event toolbar.

To print multiple events

1. In the search results screen, select the check boxes for the events you want to print.
2. Click the Printable View button in the results toolbar. Find this at the top of the page.

Review Quarantined E-mails

Quarantined events are any e-mails that require approval from a manager before they can be delivered to their intended recipient(s). For example, NYSE rule 472 stipulates that certain categories of documents sent to multiple external recipients must be approved by an appropriate representative; the iConsole enables your organization to enforce this requirement.

To review quarantined e-mails

1. Go to the Review tab.
2. In the left pane, expand the Searches group and run the Quarantine Search.

   Note: You can first refine the search using the Properties button  .
3. In the Audit pane of the search results screen, you can:

   Release From Quarantine

   Click the Release button  to allow the e-mail to be sent to its recipient(s). This option requires that a Quarantine Manager is installed and correctly configured. For details, refer to the *Platform Deployment Guide*; search for 'Quarantine Manager'.

   Reject From Quarantine

   Click the Reject button  to remove the e-mail from the quarantine list and effectively block it. That is, it is not sent to its recipient(s).

   If the administrator has configured the Administration console event audit options to make comments optional or mandatory when releasing or rejecting an event from quarantine, a dialog box appears enabling you to add a comment.

   Note: You cannot add a new issue to a quarantined event until the event has been released or rejected from its quarantined state.

Capped Searches

By default, iConsole searches are capped. This means, for example, that a search may only return 100 results even if there are more events than this in the CMS database that match the search criteria.

Because searches are typically capped, you must specify the **query sort order**. This determines the order in which the iConsole retrieves events from the CMS database.

If required, you can override the search capping to run a search of unlimited size.

Why are Searches Capped?

Typically, iConsole searches have both an administrator-defined limit and a lower limit defined by the reviewer running the search:

- By default, iConsole searches are limited to a maximum of 1,000 results. This prevents very large searches from consuming excessive memory and adversely affecting iConsole performance for all logged-on users.

  Administrators can reset this limit by editing the MaximumResultSetSize registry value. For details, see the *Platform Deployment Guide;* search for 'iConsole: search results, configuring'.

- In addition, each iConsole search has a Maximum Results limit, which defaults to 100 and is defined in the Search Properties page.

  This default limit means, for example, that a search can only retrieve a maximum of 100 results. This maximum limit prevents a search from taking too long. However, you can raise the Maximum Results when you customize a search.

- If you set the Maximum Results higher than the administrator-defined limit (see above) and you are permitted to run unlimited searches, a hyperlink is appended to the results count in the results page, enabling you to retrieve the full results.

Set the Query Sort Order

If your search is capped (that is, it is only permitted to return a subset of results), you need to specify the **query sort order**. This determines whether CA DataMinder retrieves the oldest or most recent events that match the search criteria.

Important! Do not confuse the query sort order with the **display sort order,** which determines the order in which events are displayed in the Search Results page. For example, you can display search results by time stamp, in descending order.

To set the query sort order

1. Go to the Review tab.
2. In the left pane, expand the Searches list.
3. In the right pane, click Properties  to customize a search.

   The Search Properties screen displays.
4. In the Settings tab, specify the Query Sort Order. The following options are available:

   Unsorted

   Retrieves the first events found that match the search criteria. The order in which the database is searched depends on the combination of search filters. In effect, this option retrieves events in a random sort order. But it does produce a faster search than the Most Recent First or Oldest First options.

   Choose Unsorted if you know that the search will only return a small number of events (that is, less than the maximum number permitted by the search cap).

   Most Recent First

   Retrieves the most recently captured events that match the search criteria.

   Oldest First

   Retrieves the oldest events in the database that match the search criteria.

More information:

Capped Searches (see page 54)

Run an Unlimited Search

By default, iConsole searches are capped. This means, for example, that a search may only return 100 results even if there are more events than this in the CMS database that match the search criteria. However, it is possible to run unlimited searches. That is, the iConsole will return all events that match the search criteria.

Requirements

- Your iConsole server must be configured to support unlimited searches. This is determined by a registry value, AllowUnlimitedSearches; see the *Platform Deployment Guide* for details.
- You must have the 'Events: Allow searches of unlimited size' administrative privilege to get unlimited results. See your iConsole administrator if you require this privilege.

To run an unlimited search

1. Run the search.

   The Search Results page shows matching events up to the Maximum Results limit defined in the Search Properties page. For example, the results count may show '1 to 25 of 100'.

   If the Maximum Results limit is higher than the administrator-defined search limit, the Search Results page also displays a Show More hyperlink. The tooltip for this hyperlink reads 'Get more results up to the system cap (1000)'.

2. Click the Show More hyperlink.

   The Search Results page now shows matching events up to the administrator-defined limit (defined in the registry). For example, the results count may show '1 to 25 of 1000'.

   If the requirements for unlimited searches are met (see above), the Show More hyperlink is still displayed, but now its tooltip reads 'Get unlimited results'. In addition, a 'Capped' label is shown next to the results count.

   Note: Unlike in previous versions of CA DataMinder, the 'Capped' label is *not* a hyperlink.

3. Click the Show More hyperlink again.

   Before the full search count is displayed, a warning dialog is displayed. This indicates that running an unlimited search may slow performance for other iConsole users.

4. Click OK to clear the dialog and proceed to the Search Count page. This gives the full number of matching events and estimates the time needed to retrieve these events from the CMS.

5. If the time estimate is acceptable, click Continue to retrieve the full (that is, uncapped) search results.

   For example, the results count may now show '1 to 25 of 3829'.

More information:

Capped Searches (see page 54)

Content Searches

Content searches use intelligent pattern-matching technology to analyze the text content of indexed events in a content database and retrieve events that match the search criteria. Content searches are available in the iConsole and Data Management console.

Content searches offer several advantages over standard CA DataMinder searches. You can specify the usual search criteria (event type, user or group, when the event was captured, and so on). But you can also search for specific text content and sort the search results by relevance. You can include logical operators in your search expression to zero in on key documents and eliminate irrelevant results. You can even search for documents with common themes or concepts.

Note: Content searches are only if available if included in your license agreement.

Why Use Content Searches?

The iConsole and Data Management console already offer a range of standard searches that you can easily customize. So why use content searches? Because they offer offers powerful search functionality that far exceeds that offered by the standard searches. In particular, content searches can do the following.

Analyze the Text Content

Most importantly, and as the name implies, content searches can analyze the text content of captured e-mails and files.

Standard searches cannot do this. They only allow you to search by event attributes such as the URL or e-mail address, the time of capture, or name of the associated user.

Rank Search Results by Relevance

Content searches can assess and rank the relevance of individual documents. They can also ignore documents that contain a keyword but which are otherwise unrelated to the main search 'theme'.

Include Logical Operators in Search Terms

The search term refers to the words or phrases that you are searching for in a document. When you define the search term for a content search, you can include logical operators (such as AND, OR, and NOT) to search for contextualized occurrences of keywords or phrases.

Before You Start

Content searches utilize the intelligence held in a content database. But before you can run a content search, you must populate the content database with CA DataMinder events. The content database then processes these events, storing them as indexed, text-searchable documents. When you run a content search, the content database analyzes the indexed documents and returns all documents that match the search term.

To populate the content database, use the content indexer utility. Full instructions are in the content indexer online help.

Run a Content Search

The iConsole Review tab lists the available content searches.

To run a content search

1. Go to the Review tab.
2. Click the Searches link.

   The Searches page lists the available searches.
3. Identify the content search that you want and click Actions, Edit Properties.

   The Properties screen displays. Settings are grouped into tabs, such as Basic Filters and Identity.
4. Customize the search properties as required. In particular:
   - Specify the **Search Term** in the Basic Filters tab.

     The search term defines the words or phrases that you want to find. You can use wildcards, logical operators and other modifiers when defining the search term.
   - Specify the **Confidence Level** in the Settings tab.

     The confidence level is a percentage estimate of how relevant a document is to the main search theme. You specify the minimum confidence level for documents included in the search results.
5. Click the Save or Save and Run buttons to save your changes.
6. Click the content search you want to run.

Logical Operators in Search Terms

When defining content search terms, you can use logical operators such as AND and NOT. These operators give you enormous flexibility to refine or modify your searches. They allow you to pinpoint the items that really interest you and eliminate the items that do not.

Available Operators (AND, NOT, OR and so on)

CA DataMinder content searches support the following logical operators in search terms.

Boolean Operators

Use these operators to refine your search terms by applying Boolean conditions to keywords.

AND

This operator links two search terms. Both must occur in a document to confirm a match. The order in which the terms appear is not important. AND must be in uppercase.

Example: The following search term only returns documents containing both *Unipraxis* and *complain*:

```
Unipraxis AND complain
```

NOT

This operator applies to a single term. The term must not occur in the document. If it does occur, no match is confirmed. NOT must be in uppercase.

Example: The following search term only returns documents if they contain no mention of *UXLogiCard*:

```
NOT UXLogiCard
```

OR

This operator links two search terms. If either or both occur in a document, a match is confirmed. If neither occurs, no match is confirmed. OR must be in uppercase.

Example: The following search term returns any document containing *takeover* or *acquisition*, or both:

```
takeover OR acquisition
```

EOR or XOR

This is an Exclusive OR operator. If either search term (but not both) occur in a document, a match is confirmed. If both or neither occur, no match is confirmed. EOR or XOR must be in uppercase.

Example: The following search term returns any document containing either *UXLogiCard* or *UXProPack*, but not both:

```
UXLogiCard EOR UXProPack
```

Proximity Operators

These operators enable you to filter to content searches based on the proximity of keywords to each other within a document.

NEAR*n*

This operator allows you to retrieve documents based on the proximity of two terms within a document. If two keywords appear close together in a document (say, in the same sentence), this increases the likelihood that they are conceptually linked and not just random, unrelated occurrences within the document. The order in which the terms occur is not important.

If the second term is within *n* words of the first term, a match is confirmed. If either term is absent, or if the number of words separating the two terms is greater than *n*, no match is confirmed. The order in which the terms occur is not important. NEAR must be in uppercase; *n* is a number.

Example: The following search term returns any document containing such phrases as *Unipraxis are planning an imminent takeover*:

```
Unipraxis NEAR6 takeover
```

Note: If you do not specify a number, NEAR assumes a five word gap (equivalent to NEAR5).

DNEAR*n*

DNEAR*n* is a directional variant of NEAR*n*. For this operator, the order of the two search terms is important. For a document match to be confirmed, the second term must follow the first term within *n* words. DNEAR must be in upper casein uppercase.

Example: The following search term looks for documents where *UXLogiCard* occurs no more than 10 words after the word *complain*.

```
complain DNEAR10 UXLogiCard
```

Note: If you do not specify a number, DNEAR assumes a five word gap (equivalent to DNEAR5).

WNEAR*n*

WNEAR*n* is a weighted variant of NEAR*n* with an OR condition.

WNEAR returns documents that contain either of the two terms. However, a document's confidence level is raised when the gap between the two terms is the same or less than the gap specified by *n*. In other words, the closer the terms occur within a document, the more likely the document is to be relevant. WNEAR must be in upper casein uppercase.

Example: The following search term looks for documents that contain *UXLogiCard or UXProPack.* A higher confidence level is given to documents in which *UXLogiCard or UXProPack* occur six or fewer words apart. Documents that contain only one term, or where the gap is more than six words, are assigned a lower confidence level, because these documents are less relevant to the search.

```
UXLogiCard WNEAR6 UXProPack
```

Note: If you do not specify a number, WNEAR assumes a five word gap (equivalent to WNEAR5).

YNEAR*n*

YNEAR*n* is a weighted variant of NEAR*n* with an AND condition.

WNEAR returns documents that contain both of the terms. However, a document's confidence level is raised when the gap between the two terms is less than the gap specified by *n*. YNEAR must be in uppercase.

Example: The following search term looks for documents that contain *UXLogiCard* and *UXProPack.* A higher confidence level is given to documents in which *UXLogiCard* or *UXProPack* occur less than six words apart. The confidence level increases as the terms get closer together, because these documents are more relevant to the search.

```
UXLogiCard YNEAR6 UXProPack
```

Note: If you do not specify a number, YNEAR assumes a five word gap (equivalent to WNEAR5).

XNEAR*n*

XNEAR*n* returns only documents where the two terms are exactly *n* words apart.

Example: The following search term only returns documents in which *UXProPack* occurs exactly two words after *UXLogiCard.* This means that documents containing *UXLogiCard and UXProPack* are returned in the search results. Conversely, documents containing *UXProPack and UXLogiCard* or *UXProPack, UXLogiCard* are not returned.

```
UXLogiCard XNEAR2 UXProPack
```

BEFORE

This operator applies to two search terms. The order in which the terms occur is important. For a document match to be confirmed, the second term must follow the first. If the second occurs before the first, no match is confirmed. BEFORE must be in uppercase.

Example: The following search term looks for documents where the word *complain* occurs before *UXLogiCard*.

```
complain BEFORE UXLogiCard
```

AFTER

This operator applies to two search terms. The order in which the terms occur is important. For a document match to be confirmed, the first term must follow the second. If the first occurs before the second, no match is confirmed. AFTER must be in uppercase.

Example: The following search term looks for documents where *UXLogiCard* occurs after *complain*.

```
UXLogiCard AFTER complain
```

SENTENCE

This operator applies to two search terms. It returns only documents in which the second term is in the same sentence as the first term.

Example: The following search term only returns documents in which *Unipraxis* and *takeover* occur in the same sentence:

```
Unipraxis SENTENCE takeover
```

PARAGRAPH

This operator applies to two search terms. It returns only documents in which the second term is in the same paragraph as the first term.

Example: The following search term only returns documents in which *Unipraxis* and *takeover* occur in the same paragraph. These terms do not need to be in the same sentence.

Unipraxis PARAGRAPH takeover

Search Term Modifiers

If you use logical operators, you can use the following methods to modify the search term.

*** wildcards**

Use * wildcards to define search terms. For example, this search term returns documents containing words such as *UXLogiCard* or *UXProPack*:

UX

Exact Phrases

Search for exact phrases by enclosing them in double quotes. For example:

```
"UXLogiCard upgrade offer"
```

Brackets ()

Use brackets to define subexpressions. This example returns documents in which *complain* occurs before *UXLogiCard* or *UXProPack:*

```
complain BEFORE (UXLogiCard OR UXProPack)
```

Note: Logical operators are evaluated left to right unless brackets are used

Line breaks

Add line breaks to make complex search expressions easier to read. For example:

```
complain BEFORE
(UXLogiCard OR PraxisPro)
```

Example Search Term

This example illustrates the use of multiple operators in a complex search expression. This expression searches for e-mail requests from customers who, after evaluating a specific product, wished to go ahead with the purchase. Logical operators are evaluated left to right unless brackets are used:

```
evaluation WNEAR6 (UXProPack OR UXLogiCard)
AND (licens* OR purchas*)
AND NOT complain*
```

Specifically, the search term detects e-mails that:

- Refer to an *evaluation* of the UXLogiCard or the UXProPack products.
- Contain a word such as *licensing* or *purchase*.
- Do not contain words such as *complain* or *complaint*.

For example, the following customer request meets all of the above criteria:

```
Hi guys,

We've now completed our evaluation of UXProPack1. The product looks great and we
want to buy!
I have a question about licensing. What's the best deal can you do us for 250
desktops?

Look forward to hearing from you,
Tarquin, MIS Manager
```

Confidence levels

A CA DataMinder content database differs from a conventional relational database. All documents stored in the content database are rigorously dissected and indexed. As the database accumulates data, it acquires a sophisticated understanding of these documents based on content analysis that can contextualize occurrences of individual words within a document. This enables it to identify clusters of related documents, defined by their characteristic text patterns that reveal a shared subject or theme.

When you run a content search, the content database uses its acquired expertise to discern the theme embodied by your search criteria. It then examines each matching document for the text patterns that characterize this theme. For example, if you search for occurrences of the word 'sales', the content database compares each matching document against the characteristic profile of other sales-themed documents in the Content database.

By calculating the comparative strength of the various text patterns discernible in a document, the content database is able to quantify how closely it matches a particular theme. It then generates a percentage probability that the document corresponds to a specific theme. This probability is the confidence level.

When you run a content search, you specify a minimum confidence level. Documents that meet the search criteria but which do not have a high enough confidence level are considered irrelevant to the search. This eliminates false hits and focuses the search on documents that are relevant to the search theme.

Bookmark a Search

You can add any search to Favorites in your browser to quickly and easily re-run regular searches.

To add a search to your Favorites

1. Go to the Review tab.
2. In the left pane, expand the Searches group.
3. Click Add to Favorites  for the search you want.

Derive a New Search

A derived search is similar to a customized search in that both are variations of an existing search. But unlike normal customized searches, derived searches can be published and made available to users.

It is also possible to edit the XML definition file of a derived search, allowing you to change text labels and default parameter values. In addition, unlike normal customized searches, a derived search can be based on an unpublished existing search. This is useful, for example, if you want users to use a modified version of the default iConsole Standard Search but without the 'real' Standard Search being available to them. For full implementation details, see the *iConsole Search Definition Guide*; search for 'derived searches'.

To derive a new search from an existing search

1. Go to the Searches page in the Administer Searches tab.
2. In the Manage Stored Searches screen:
   a. Select the check box for the search you want.
   b. From the Actions menu for that search, choose Edit Properties.
3. Edit the search properties as required.

   For example, choose which columns to show in the results screen. You can also click Customize to hide or unhide available search parameters.
4. Click Save to save the customized search.
5. In the Save Search dialog, enter a name and description for the modified search.
6. Edit the underlying XML search definition.

   See the next section.

To edit the XML search definition

Not all search modifications can be made directly in the iConsole. If you want to change the text labels for search parameters or amend other parameter attributes, you need to edit the underlying XML in the new definition file.

1. In the Manage Stored Searches screen:
   a. Select the check box for the search you want.
   b. From the Actions menu for that search, choose Export.
2. Use an XML editor to make any required changes.
3. Now re-install the modified XML search definition file.
4. In the Manage Stored Searches screen, click Install.
5. In the Install Searches dialog, specify the XML file you modified in step 2.

The new derived search, including the latest XML modifications, is added to the Searches folder.

6. Test the new search to confirm that it returns results as expected. To do this.
   a. In the Manage Stored Searches screen, select the check box for the search you want.
   b. From the Actions menu for that search, choose Test
7. Publish the new search. To do this.
   a. In the Manage Stored Searches screen, select the check box for the search you want.
   b. From the Actions menu for that search, choose Publish.

   When you publish a new search, it becomes available to all other iConsole users and is listed in the Review tab.

Troubleshooting Event Searches

Event Searches

When you search CA DataMinder for captured events, the search can sometimes find no matching events even when you know such events exist in the CMS database.

There are several possible reasons why this happens:

- You have not created a Search User database account. The iConsole needs two user accounts that it can use to access the CMS database. The first is the Primary User, specified when you install the CMS. The second is the Search User, used by the iConsole. This is a secure database account that is used to search the database for events. Without a Search User, reviewers will be unable to retrieve events. For details, see the *Database Guide*; search for 'search user'.
- None of the event's associated users are mapped to iConsole users. For example, this can happen if you import e-mails or IM data but fail to keep e-mail addresses for your iConsole users up to date. In this situation, the iConsole may be unable to map an event's associated users to existing iConsole users.
- None of the iConsole users that are mapped to the event's associated users fall within your management groups. You can only retrieve search results for users belonging to groups within your management branches.
- Although one of the users mapped to the event's associated users is in your management group, they were not when the event was captured or imported. Management group boundary enforcement is based on the user group of the event's associated users at the time of capture. For example, if an e-mail sender was not in your management group when the e-mail was captured, you cannot search for that e-mail at a later date, even if the sender has subsequently been moved into your management group.

  Note: To override management group constraints, you can assign the Admin: Disable management group filtering privilege to an administrator. For details, please refer to the *Administrator Guide*; search for 'searches, no matching events returned'.
- The events you are searching for have already expired. That is, their minimum retention period has expired and they have been purged from the CMS database.
- The event you are searching for has a capture date in the future. Such events are excluded from search results until after the capture date. This can only happen if the system clock is set to the wrong date on the relevant source machine (for example, a client machine hosting the Outlook client agent or, for imported e-mails, the sender's machine).

Microsoft IE Limitation

Internet Explorer (version 7 or higher) enables you to view multiple Web sites in a single browser window using tabs. In the iConsole, if a user tries to log in as different users in two of these tabs, then the session login details of the iConsole in the first tab is overwritten. This is because IE tabs share session cookies and so tabs must share the session for a particular domain or URL. It is therefore not possible to use Internet Explorer tabs to log in as different users.

Chapter 6: Running a Report

This section contains the following topics:

Available Reports

The available standard reports are summarized in the following sections.

Compliance Reports

These include:

Compliance Audit Report

Shows workload statistics for each reviewer in your management group(s). It shows the number of events allocated to each reviewer and the number already reviewed over a specified period. Optionally, it also indicates how long reviewers spend reviewing individual events.

Employees Not Reviewed Report

Lists users who have not had any of their associated events reviewed over a specified period. A 'reviewed event' is an event with one or more issues.

Proof of Supervision Report

Shows reviewed events as a percentage of all captured events, by user or group.

Repeat Offender Report

Shows the number of incidents associated with each 'offender'. An offender is any user associated with an issue. They can be the sender or a recipient of the message.

Review Latency

Shows the level of events that are still unreviewed. The report identifies the reviewers and the user groups associated with the unreviewed events. It also indicates how many days these events have been waiting to be reviewed. Percentage scores allow you to compare review rates by reviewer or/and user group.

Reviewer Activity

Shows the activity of individual reviewers in terms of the number of events viewed and audited. This report enables managers to monitor reviewer activity and, if necessary, confirm that events are being audited correctly.

Note: These reports are not designed for use with Policy security models. See the reference below for details.

More information:

Policy Security Models Not Compatible With Some Reports or Review Queue (see page 81)

Incident Reports

These include:

Incident Rate By Policy Report

Shows a breakdown of all the policies that have been triggered over a specified period, showing their counts as a percentage of all events processed. By default, it includes all policies, but it can be refined to focus on just a subset. It calculates percentages based on all events in the database captured over the specified period.

Incident Summary Report

Shows how many times a user (employee) has caused a trigger to fire during a specified period. You can use this report to search for details of captured events associated with a specific user, group or trigger, incoming or outgoing events, or events captured over a specific period.

Incidents By Location Report

Provides a summary of 'Data At Rest' trigger violations by file location (that is, the host machine and folder containing the file). It shows the number of incidents for each file location.

Incidents By Policy and Action Report

Shows how many file policies were triggered and the subsequent actions (for example, capture, delete, move, or copy a file).

Incidents By Policy and Channel Report

Shows the number of violations by policy or class for specific users or groups, broken down by channel. For example, it shows how many violations were caused by emails, FTP transfers or instant messages. Reviewers can analyze the results to see which policies trigger most often and on which communication channels.

Incidents By Policy and Time Period Report

Shows the number of violations over time broken down by policy or class, for specific users or groups. For example, it can show changing violation counts on a weekly or monthly basis. Reviewers can analyze the results at a policy or class level to understand the overall trend over time.

Incident Cause Frequency Report

Shows incident counts for specific policy conditions: Parameter 7 words detected by a Document Classifier trigger; e-mail senders; and e-mail subject lines. This diagnostic report is designed for policy administrators. It allows them to understand how policy is being applied to real data and, if necessary, to fine tune those policies to reduce false positive results. Note that you can also drill down into the results to see the individual events.

Issue Reports

These include:

Detailed Issue Report

Lists current details for individual issues, including audit status and resolution, reviewers, and associated users.

Issues By Status or Resolution Report

Shows the number of issues for specific users or groups, broken down by audit status or resolution. For example, reviewers can see the number of issues with an audit status of 'Escalate' or 'Pending' for events captured in the last month.

Review Queue

The Review Queue feature is optional. It includes the following administrative reports:

Review Queue Configuration

Shows the event selection rules for your management groups when a review queue job runs.

Review Queue Diagnostics

Provides details about the most recent review queue run. For each step, it shows the execution time, the actual query statement and the status.

Review Queue History

Shows summary details for previous database review queue runs, including run times, status and event counts.

Note: For instructions on how to customize and manage the Review Queue, see the *Review Queue Implementation Guide*. This is available to download from CA Technical Support.

More information:

Policy Security Models Not Compatible With Some Reports or Review Queue (see page 81)

BusinessObjects Enterprise Reports for CA DataMinder

(Available only if CA DataMinder integration with BusinessObjects Enterprise is enabled.)

The BusinessObjects page of the Review tab shows the following items:

InfoView link

InfoView is the BusinessObjects web portal. Click the link to open an InfoView window.

CA DataMinder Reports

The reports are versions of the following standard CA DataMinder reports redesigned for BusinessObjects:

- Compliance Reports (see page 74)
- Incident Reports (see page 75)
- Issue Reports (see page 76)

This folder maps directly to the CA DataMinder folder in the InfoView Document List.

Inbox

The inbox includes scheduled BusinessObjects reports for CA DataMinder that ran successfully.

My Favorites

This folder includes your customized versions of BusinessObjects reports for CA DataMinder.

This folder maps directly to the following folder in InfoView: \All\My Favorites.

Note: If you want your customized reports to be listed in this 'My Favorites' folder in the iConsole, you must save them to the \All\My Favorites in InfoView.

Run a Report

Available reports are in the iConsole Review tab.

To run a search

1. Go to the Review tab.
2. In the left pane, expand the Reports group.

   The right pane shows summary details for available reports. Icons identify the report type:

    **Predefined** reports are available to all users logged on to the CMS.

    **Customized** reports are your own saved and customized reports. They are not available to other users.

    **Derived** reports are customized reports available to all users.
3. Click the report you want to run.

Customize a Report

You can customize any existing report. For example, you may want to change the date range. When you customize a report, it is added only to your reports list, it is not available to other users.

To customize an existing report

1. Go to the Review tab.
2. Click the Reports tab.
3. Click Actions, Edit Properties to customize a report.

   The Report Properties screen displays. Settings are grouped into tabs.
4. Customize the report properties as required.
5. Click the Save or Save and Run buttons to save your changes.
6. Enter a name and description for the customized report.

   Your new customized report  is added to your Reports list.
7. Click the Action button to rename or delete customized reports.

BusinessObjects Reports for CA DataMinder

CA DataMinder can integrate with BusinessObjects Enterprise, allowing you to run and customize BusinessObjects reports for CA DataMinder.

Why Run BusinessObjects Reports?

CA DataMinder integration with BusinessObjects Enterprise has several advantages:

- A BusinessObjects report is generally faster than a corresponding standard CA DataMinder report. For example, the BusinessObjects version of the Issues By Status or Resolution report returns results much faster than the corresponding standard CA DataMinder report.
- BusinessObjects Enterprise is a leader in enterprise reporting systems. It enables users to create their own reports in a user-friendly interface and to specify the report output format (such as Excel or PDF). It also supports automated scheduling and distribution of reports.
- If you already use BusinessObjects Enterprise to run reports for other CA products such as SiteMinder or Identity Manager, your managers and administrators can use the BusinessObjects web portal, InfoView, to manage all their CA reports, including CA DataMinder reports, in a single customizable web interface.

How Do Users Run BusinessObjects Reports for CA DataMinder?

You can access BusinessObjects reports for CA DataMinder in the following ways:

- Directly from the iConsole. You can browse to CA DataMinder iConsole and run BusinessObjects reports directly from the Review tab.
- Launching InfoView from a link in the iConsole. You can then create, schedule and run CA DataMinder reports from the portal.
- Browsing directly to InfoView. As above, you can then create, schedule and run CA DataMinder reports from the portal.

Launch InfoView

You can launch InfoView from the iConsole or you can browse to InfoView directly.

Note: In BusinessObjects XI 3.1 SP3, InfoView is not supported in Microsoft Internet Explorer 9.

To launch InfoView from the CA DataMinder iConsole

1. Log on to the iConsole using an account that can connect to BusinessObjects Enterprise.
2. Go to the iConsole Review tab.
   - If trusted authentication **is** enabled and your CA DataMinder account matches an existing BusinessObjects account, the Review tab displays automatically.
   - If trusted authentication is **not** enabled or your CA DataMinder account does not match an existing BusinessObjects account, the BusinessObjects Enterprise Login dialog appears.

   Note: Trusted authentication allows users to log on to a system once, without needing to provide passwords several times during a session. In the case of CA DataMinder and BusinessObjects Enterprise, it means that users do not need to log on separately to BusinessObjects when they run a BusinessObjects report or launch InfoView from the iConsole.
3. (Applicable only if the BusinessObjects Enterprise Login dialog appears) Enter the user name and password of a BusinessObjects Enterprise account and click OK.
4. Go to the BusinessObjects page in the Review tab.

   The BusinessObjects page includes a link to InfoView.
5. Click the InfoView link.

   The InfoView home page displays.

To launch InfoView directly

Browse to the InfoView URL. This URL has the following format:
`http://<BOE Server>:<WebApp Port>/InfoViewApp`

Where <BOE Server> is the BusinessObjects Enterprise host server and <WebApp Port> is the connection port for the web application server that runs InfoView. The default port Is 8080. For example, if BusinessObjects Enterprise is hosted on UX-ReportsSvr-W2K8, the InfoView URL is:
`http://UX-ReportsSvr-W2K8:8080/InfoViewApp`

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.

Chapter 7: Dashboards

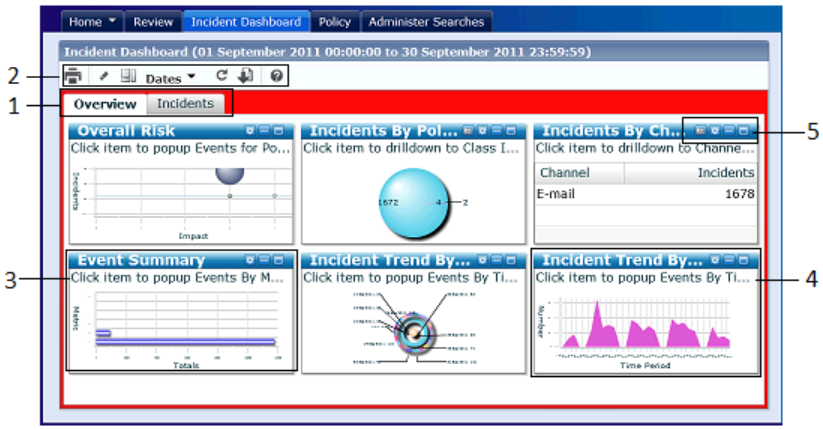
This section contains the following topics:

About Dashboards

The iConsole dashboard shows charts and metrics of incidents and violations, broken down by policy, channel or impact. Data is shown in separate panes which you can configure and rearrange to focus on the areas of most interest.

You can also drill down into a pane to view a list of the underlying events or, for pie charts, a further chart showing a breakdown of the data in an individual pie slice. Likewise, in a 'table' pane you can click individual cell values to view the underlying incidents.

Note: Dashboard charts and metrics are based on aggregated data.



Example dashboard layout

1. **Page tabs:** Click to switch between dashboard pages.
2. **Dashboard configuration buttons:** Use these buttons, for example, to update the dashboard to use the latest available data, or to reset it to its original layout, or to change the dates.
3. **Metrics pane:** These summarize the number of blockings and warning, reviewed and unreviewed incidents, and escalated incidents, for the current time period. Click any metric to drill down and see the underlying individual incidents.
4. **Chart pane:** The dashboard supports all common chart types, including pie charts and bubble charts. This example shows an area chart. Use the pane options (4) to configure the chart.

   Hover over a data point to see summary details. Click any data point to drill down to see the underlying data.
5. **Pane options:** Use these buttons to resize the pane and set the chart options (type, legend, axis labels, and so on).

View the Dashboard

The Incident Dashboard is installed automatically with CA DataMinder FastStart. You can save your own customized versions of it.

To view the standard Incident Dashboard

Go directly to the Incident Dashboard tab.

To view a dashboard that you have customized

1. Go to the Review tab.
2. In the left pane, expand the Dashboards group.

   The right pane shows summary details for available dashboards. Icons identify the dashboard type:

    **Predefined** dashboards are available to all users logged on to the CMS.

    **Customized** dashboards are your own saved and customized dashboards. They are not available to other users.

    **Derived** dashboards are customized dashboards available to all users.
3. Click the dashboard you want.

Dashboard Pages

You can sort and resize columns as required, and filter results by time period and date. Click any cell value or chart segment to drill down and view the underlying incidents.

The dashboard comprises the following CA DataMinder charts:

Event Summary

Metrics summarize the number of blockings and warnings, plus reviewed and new (that is, unreviewed) incidents, and escalated incidents.

Incident Trend By Impact

Shows the number of incidents over time, broken down by impact. The x-axis time period varies according to the overall dashboard time period.

Incident Trend By Policy

Shows the number of incidents over time, broken down by policy. The x-axis time period varies according to the overall dashboard time period.

Incidents By Channel

Shows the number of incidents by communication channel (for example, email, Webmail, Web pages, FTP file transfers). Click a pie segment to drill down to see incidents by policy for that channel.

Incidents by Policy

Shows the number of incidents captured by each policy. Results are broken down by impact (high, medium or low).

Incidents By Policy Class

Shows the number of incidents by class; click a pie segment to drill down to see incidents by policy for that class.

Incidents by Sender

Shows the number of captured incidents by sender. Results are broken down by impact (high, medium or low).

Overall Risk

Bubble chart shows the number of incidents per policy which have a low, medium or high impact. Bubble size indicates the number of violators (that is, individual users) associated with each incident count.

Organize Dashboard Panes

Use the pane buttons to organize the panes as required. You can drag and drop individual panes to rearrange the page layout. Alternatively, you can minimize or maximize any pane to focus on the data that interest you.

By default, the CA DataMinder Overview page contains six panes but you can minimize any of these to focus on the panes that interest you. You can also drag and drop individual panes to rearrange the page layout. Alternatively, you can maximize any pane to see the data in more detail.

Use the Refresh or Re-Run buttons to update the dashboard to use the latest available data or reset the dashboard to its original layout

Configure Chart Options

Click the Options button in any pane to select the chart type and display or hide the chart axis labels and legend. The dashboard supports all common chart types, including pie charts and bubble charts. For bar, column and area charts, you can additionally specify whether data series are shown in normal or stacked or 100% formats.

Dashboard Time Period

You can set the dashboard time period to focus on current activity or longer term trends. You can choose a predefined period (such as 'Today' or 'Last Week'), or you can specify a custom period. Note that periods such as:

- This Week, This Month or This Year mean a period beginning from the start of the current week, month or year and ending today.
- Last Week, Last Month or Last Year mean the week ending on the previous Saturday or the last calendar month or year. They do not mean, for example, the last 7, 31 or 365 days.

For trend charts (such as CA DataMinder Alert Trend By Policy), the x-axis time periods are dependent on the overall dashboard time period. For example, if the dashboard time period is set to Last Year, the x-axis aggregates incidents into monthly counts:

Dashboard time period	X-axis periods for dashboard trend chart
Year or Quarter	Months
Month or Week	Days
Day	Hours

The Blocked Incidents, Disregarded Warnings and Accepted Warnings metrics are all based on the dashboard time period. For example, if the time period is set to this month, the Blocked Incidents metric counts the number of incidents that were blocked since the start of the current month.

Dashboard History Period

The Reviewed Incidents, New Incidents and Escalated Incidents metrics are all based on the dashboard 'history' period. This is set by the HISTORY aggregation parameter.

The history period simply specifies a period in months, over which incidents are aggregated. For example, if the history period is three months, the Reviewed Incidents metric will show the number of incidents that were reviewed over the three months immediately prior to the most recent aggregation. (By default, aggregations run every hour.)

Note: Information about all aggregation parameters, and instructions for customizing aggregation schedules, can be found in reports.htm.

Customize a Dashboard

Administrators can edit pages and panes to customize the dashboard.

- A dashboard contains one to ten dashboard pages.
- A page contains one to ten dashboard panes.

The dashboard master template is the system template used to generate dashboards. You can save modified copies of the master template, but you do not modify the master template itself.

Create a Custom Dashboard

Note: You can only create a new dashboard if you have the administrative privileges Admin: Manage iConsole Searches and Admin: Allow iConsole Dashboard Searches. Privileges are granted in the Administration console.

To create a new dashboard

1. Go to the Administration tab. Under Manage Stored Searches, choose the System category, and open the Dashboard tree.
2. (Optional) Edit an existing pane (see page 89) and customize it.

   Click Save to save the pane under a new name.

3. Edit an existing page (see page 91) and add panes to the page definition.

   Click Save to save the page under a new name.

4. Edit an existing DashboardMaster and add pages.

   Click Save to save this dashboard under a new name.

5. Use the Test action to test the new dashboard.

   The dashboard opens in a new window for review.

6. Publish the new dashboard.

   The dashboard is available to iConsole users.

Edit Dashboard Pane Properties

You edit Dashboard pane properties on the Administration tab under Searches. Choose the System category and open the Dashboard section. To create a new pane, edit an existing pane and save it under a new name.

To edit the dashboard Pane properties:

1. Click Action, Edit Properties on the Pane.
2. Specify the date range.

   In Date Range:

   Set the date range for the dashboard. For example, choose 'This Month' if you want the dashboard to show results from the start of the current month up to today.

3. Click the Pane Configuration tab to configure the dashboard pane.

   Example: You can set the pane type to Chart, and then the initial Chart Type to ‘Bar’; then you select Area and Grid as Allowed Types. This pane type configuration lets the users switch to Area or Grid visualization if the initial bar chart visualization is not suitable.

   Pane Type:

   Specifies whether the pane displays data as a Chart, List or Tree.

   Chart

   Chart panes visualize data as bar, pie, column, line, bubble, area, or grid chart. If you choose the chart pane type, you must also specify the initial **Chart Type** and **Allowed Types**. This selection allows users to visualize the data as alternative chart types.

List

List panes contain lists of metrics (summary totals, such as the total number of unreviewed incidents). You define the metrics that are displayed in this list pane by specifying a database stored procedure in the Search Settings step.

Tree

Similar to list panes, tree panes contain information (such as metrics) organized hierarchically in a tree structure. You define the contents of the tree pane by specifying a database stored procedure in the Search Settings step.

Pane Attributes:

Enter the attributes of the pane, for example, chart axis type. Specify one or more attributes, for example, you can specify a logarithmic x-axis for bar charts. The supported attributes are listed in the *iConsole Search Definition Guide*; search for 'pane attributes'. Use a semicolon separated list if you specify multiple attributes

4. Click Search Settings.

Note: To maintain consistency between Oracle and SQL Server databases, dashboards assume that all pane SP names adhere to the following convention: <Package>_<Procedure>. If you implement a custom SQL Server procedure, it must adhere to this convention and you must enter the <Package> element in the SQL Package field and the <Procedure> element in the Procedure Name field. CA DataMinder infers an underscore character between these two elements.

SQL Package:

Enter the name of an SQL package containing the stored procedure. The required input for this field depends on your CMS database engine:

- Oracle CMSs: Enter the SQL package containing the database stored procedure (SP) for the current pane. For example, the SQL package name for the Incident Dashboard is DLPDASH.
- SQL Server CMSs: Enter the 'package prefix' of the SP for the current pane. For example, if your procedure is named DASH_SEVERITYPIE, enter DASH in this field. See below for naming requirements for SQL Server SPs.

Procedure Name:

Enter the name of the stored procedure to run that populates the pane. The required input for this field depends on your CMS database engine:

- Oracle CMSs: Enter the name of the SP for the current pane. This SP defines the underlying database search used to populate the pane.
- SQL Server CMSs: Enter the 'procedure suffix' of the SP for the current pane. For example, if your procedure is named DASH_SEVERITYPIE, enter SEVERITYPIE in this field. See below for naming requirements for SQL Server SPs.

5. (Optional) Specify Pane specific settings.

   Column Selector

   Select the columns that you want to display on the Search Results page. By default, all columns are displayed.

   Display Sort Order

   Select the columns to use when the result set is sorted. Specify whether you want to sort column content in ascending or descending order. Click the up and down arrows to specify the column's priority.

6. Click Save to save this configuration. Click Save and Run to save this configuration and view the results. Click Run to view the results without saving the configuration.

   The page and pane definitions are saved as search definitions (XML files) on the CMS. If you customize an existing page definition and save it with a new name, a derived search is created.

7. Click Save to save the Pane under the same, or a new name.

8. Click Actions, Publish to make the pane available to users.

Edit Dashboard Page Properties

You edit Dashboard page properties on the Administration tab under Searches. Choose the System category and open the Dashboard section. To create a new page, edit an existing page and save it under a new name.

To edit Dashboard Page properties:

1. Open the dashboard section and click Action, Edit Properties on the Dashboard Page that you want to customize.

   Specify the following dashboard properties.

   Number of Panes

   Specifies the number of panes in the current dashboard page. A page can contain up to 10 panes. The iConsole automatically adds a Pane Definition field for each pane.

   Pane <n> definition:

   For each pane in the dashboard page, choose a pane definition from the drop-down list of available definitions.

   A pane definition specifies the pane title and type (chart, list, or tree). Because all pane definitions are based on database packages, the pane definition also specifies the underlying SQL package and database SP, plus the drilldown pane definitions.

2. Click Save to save this configuration. Click Save and Run to save this configuration and view the results. Click Run to view the results without saving the configuration.

   The page and pane definitions are saved as search definitions (XML files) on the CMS. If you customize an existing page definition and save it with a new name, a derived search is created.

3. Use the Actions menu to test and publish the new derived page and make it available to users.

Dashboard Event Totals Seem Wrong After Drilling into Report or Chart

In certain conditions, if a reviewer drills down into a report or dashboard chart, the number of results does not match the event total shown in the report or chart. This apparent disparity can occur if further events have been captured or reviewed in the intervening period since the snapshot totals were last calculated.

Snapshot totals are recalculated each time a data warehousing job runs. By default, these jobs run every hour. Consequently, snapshots (such as 'total unreviewed events') reflect the total number of events *at the time when the job ran*.

If the number of events (or incidents) in the CMS database rises or falls before the next data warehousing job runs (for example, because a manager reviews some previously unreviewed events), then the snapshot total shown in the report or dashboard will no longer tally with the actual number of underlying events in the CMS database. If a reviewer were to drill down into the report or dashboard at this point, they would see an apparent disparity in the number of events.

Example

Consider this timeline:

15:00 PM	A data warehousing jobs finds 100 unreviewed events and adds them to the data warehouse.
15:15 PM	A manager refreshes their dashboard. The snapshot total for Unreviewed Events is 100.
15:16 PM	The same manager drills down into the dashboard to see the underlying events. The Search Results screen does indeed find 100 unreviewed events.
15:30 PM	A reviewer audits 25 of the unreviewed events in the iConsole.
15:45 PM	The manager refreshes their dashboard; the snapshot total for Unreviewed Events is still 100. This is because there has been no new data warehousing job since 15.00 PM.

15:46 PM	The manager drills down into the dashboard again. But this time, the Search Results screen only finds 75 unreviewed events!
16:00 PM	The next data warehousing job runs and finds 75 unreviewed events. The snapshot total and number of underlying events are back in sync.

Note: Such potential disparities only affect snapshots of event counts based on audit status. They cannot occur with snapshots based on non-changing event attributes such as events counts by policy.

Chapter 8: Auditing Events

This section contains the following topics:

Event Issues

An *issue* represents a specific problem or concern identified by a reviewer and associated with an event.

When you audit an event in the iConsole, any updates to the event must be attached to an *issue*. For example, you find that an email contains vulgar or obscene remarks. Consequently, you change the event's audit status from 'Deferred' to 'Not Approved' and link this change to a new issue, 'Offensive Language'. Each update to an issue is recorded in the issue history.

When you select an event in the search results page, any issues associated with the event are summarized in the right-hand pane at the bottom of the page. You can view and update the issue's history. For example, you can add comments and change the Action Taken field. You can also change the users associated with an issue. For example, you may want to associate an email issue with the sender only, so absolving the recipient.

Note: Changes to an event's expiry date are *not* attached to an issue.

Multiple Issues Per Event

A single event can breach more than one rule. That is, it can have multiple issues (for example, 'Suspected insider trading' *and* 'Offensive language'). The iConsole allows reviewers to assign multiple issues to individual events, so that each issue can be separately escalated and tracked. Each issue is assigned a name and specifies the event's associated user(s) and the issue's audit history. For example, an 'Offensive language' issue may only refer to an e-mail sender, but a 'Suspected insider trading' issue may refer to both sender and recipients.

Note: The iConsole audit features are configured in the Administration console. For example, you can set up the audit buttons  to assign the same issue type to multiple events simultaneously. For details, see the *Administration Guide*.

Create a new issue

A single Web page, e-mail or IM conversation, can breach more than one rule. That is, it can contain multiple compliance issues, for example, 'Suspected insider trading' and 'Offensive language'.

Reviewers can assign multiple issues to individual events, so that each issue can be separately escalated and tracked. Each issue is assigned a name and specifies the event's associated users and the issue's audit history.

For example, an 'Offensive language' issue may only refer to an e-mail sender, but a 'Suspected insider trading' issue may refer to both sender and recipients.

You can use audit buttons to assign the same issue type to multiple events simultaneously. These buttons are configured in the Administration console and allow reviewers to instantly change specific audit details from one value to another. For details, see the *Administration Guide*.

To create a new issue

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click the New Issue button  in the event toolbar.

3. Specify the issue name, status, action, resolution and comment In the New Issue dialog.

More information:

Multiple Issues Per Event (see page 96)

Edit an Issue

You update issues associated with an event to reflect recent developments. For each issue, you associate users and other incidents, and you specify the status, classification, action, and resolution.

From the View issue dialog, you can also add a comment, send an email to associated users, and inspect the issue history.

To update an issue

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. In the Audit pane, click View Issue next to the issue that you want to update.

   The View Issue dialog opens.

3. Make you necessary changes and (optionally) add a comment.
4. (Optionally) Click Send Email to compose a message to the originator and the users associated with this issue. You can attach the original file that prompted the event, or a link to it.
5. Click OK to update the issue with your changes.

More information

Multiple Issues Per Event (see page 96)
Audit Settings (see page 23)

View Event History or Issue History

Several auditors may be updating the same issues and events. Before you modify the event or an issue, you want to inspect their history.

To see changes to the expiry date, and see when and by whom the event was last viewed, use the event history.

To view the event history:

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. View the event history in the bottom right of the Audit pane.
3. Click View Item

   The History dialog lists recent actions for this event.

4. Click Close.

To inspect the time and author of changes to classification, approval status, associated users, action, and resolution of the issue, use the issue history.

To view the issue history:

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click View Issue next to an issue.

   The Edit Issue dialog opens.

3. Click History...

   The Issue History window opens and lists a log of all changes.

4. Click Close, and then click Cancel.

More information

Multiple Issues Per Event (see page 96)
Audit Settings (see page 23)

Bulk Auditing Events

The audit buttons  in the Search Results screen allow rapid bulk auditing. They enable you to quickly update multiple events without needing to view the events first. If the same audit change is applicable to multiple events, you can update the relevant issues for all the events with just one click of a button.

Note: If an appropriate issue does not exist, an audit button can be reconfigured to create the issue automatically.

Examples

A reviewer sorts a set of search results by Subject and notices a number of events with the same Subject. It is clear that events comprise a single e-mail thread between two employees. After reviewing the final reply in the thread, the reviewer knows the preceding replies are benign and so approves all the events in the thread by selecting the event check boxes and clicking the 'Approve' button.

Often, the same events are ingested into the CMS from multiple Policy Engines, and are displayed as multiple duplicate rows in the iConsole. You can customize a standard search to list duplicate events with specific criteria, and group these duplicates together.

A de-duplication search saves you the effort of identifying and handling duplicate events. You create and run your custom search, select a parent event, and apply audit actions (including print, review, escalate) to its child events in bulk.

More information:

Bulk Audit Duplicate Events (see page 36)

Send an Audit E-mail

The iConsole supports event escalation. You can forward selected events (as 'audit e-mails') to colleagues for further attention. You can also forward e-mails back to the original sender if, for example, they need to amend their original message before resending it.

When you forward an event, it is sent as an attachment to the audit e-mail. A 'compose' dialog enables you to write an accompanying message when you send an audit e-mail.

Note: To match your organization's terminology and requirements, administrators can define e-mail templates for reviewers to choose from. For details, see the Administration console online help; search for 'audit e-mails'.

To send an e-mail

1. Click an event title in the search results screen.

   The event details and event toolbar are shown at the bottom of the screen.

2. Click the Send Mail button  .

3. In the Compose Mail dialog, you can manually specify the recipients, the subject and body text, or you can load a predefined template. You can also add the original message.

   Add Recipients

   Type the recipient addresses directly, or click the To, Cc or Bcc buttons to pick recipients from an address book or from CA DataMinder user groups.

   Click the Add Sender button  to add the original sender to the recipients list.

   Load a mail template

   Click the Choose Template button. Templates can include predefined recipient lists, plus predefined body and subject text to match your organization's terminology and requirements.

   Add the original message

   You can add original message to your audit e-mail as an attachment; click the Attach Original button  .

   Or you can add a URL link to the event. This allows colleagues to view the event in the iConsole. Click the Include Link button  .

4. When you are ready to send the e-mail, click the Send button.

Chapter 9: Editing Policies in the iConsole

You can use the iConsole Policy tab to edit the CA DataMinder standard policies.

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

This section contains the following topics:

Available Policies

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

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

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

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

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

More information:

Corporate and Regulatory Compliance Policies

Anti-Money Laundering - OFAC

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

Bid Rigging Detection: Insurance

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

Bid Rigging Detection: Municipal Bond Issuance

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

Blast E-Mail

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

Bribes/Kickbacks/Quid Pro Quos/Blackmail

This policy detects involvement in bribery or blackmail schemes.

Broker Error

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

Communication with Regulatory, Legal, and Governmental Authorities

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

Fair and Balanced Advice

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

Information Destruction Alert

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

Investment Advice Prohibition

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

Securities Parking

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

Solicitations: Charitable

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

Solicitations: General

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

Solicitations: Political

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

Solicitations: Private Investments

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

Solicitations: Religious

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

Tax Advice Prohibition

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

Trading in an Outside Account: Order Confirmations

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

Trading in an Outside Account: Order Placements

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

Whistleblower

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

Customer / Supplier Treatment Policies

Customer Complaints: Response Prohibition

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

Customer Complaints: Unprofessional Responses

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

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

Customer Conditioning

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

Customer Threats

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

Exclusivity

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

Gifts and Entertainment

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

Guarantees and Assurances

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

Unqualified Rebates or Benefits

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

Employee Behavior Policies

Coercive Behavior and Intimidation

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

Communication with Competitors

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

Communication with the Press/News Organizations

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

Corporate Criticism

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

Deceptive Language

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

Discrimination and Racism

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

Discrimination: Age

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

Fantasy Leagues

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

Gambling Prohibition

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

Harassment

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

Inappropriate, Offensive and Sexual Language

This policy identifies communications indicative of offensive and sexual language.

Intent to Resign

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

Jokes

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

Office Relationships: Romantic

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

Outside Business Activity/Directorships/Employment

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

Termination/Layoff Discussions

Protect communications concerning potential and pending terminations and layoffs.

UK Resumes/CVs

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

US Resumes/CVs

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

Intellectual Property (IP) Policies

Confidential Trade Data

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

Patent Applications

This policy detects non public patent applications.

Product and Design Specifications

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

Proprietary Software Code

This policy detects software code, programs, and executables.

Technical Specifications or Designs

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

Legal Policies

Attorney Client Privilege

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

Discussion of Legal Proceedings

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

Potential Ethical Issues

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

Potential Legal Issues

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

Threats of Litigation

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

Non-Public Information (NPI) Policies

Board Minutes and Discussions

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

Corporate Contracts

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

Customer Lists

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

Draft Documentation

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

Financial Information - Balance Sheet

This policy detects content found on financial balance sheets.

Financial Information - Income Statement

This policy detects content found on financial income statements.

Financial Information - Projections

This policy detects the disclosure of financial projections.

Information Security Label Control

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

Inside Information: Front Running/Trading Ahead

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

Inside Information: Non-Public Company Information Loss

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

Inside Information: Non-Public Financial Information Loss

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

Inside Information: Rumors and Secrets

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

Inside Information: Trading Ahead of Research

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

Internal Investigations

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

Internal IT Support Documents

This policy identifies internal IT system and support documentation.

Licensing Agreements

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

Mergers and Acquisitions

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

Pricing List

This policy is designed to detect nonpublic pricing information.

Project Information

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

Restricted List

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

Sales Information

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

Personal Health Information (PHI) Policies

Benefits Enrollment Information

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

Diagnosis Information

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

Individually Identifiable Health Information (IIHI)

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

Medical Billings and Claims

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

Medical History

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

Medical Record Numbers

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

Medical Record Numbers - Threshold

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

Personally Identifiable Information (PII) Policies

Account Number

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

Account Number - Threshold

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

Account Number and Routing Information

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

Account Number with Additional PII

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

Australian Medicare Card Number

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

Australian State Drivers License

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

Australian Tax File Number

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

Background Checks

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

Canadian Social Insurance Number

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

Canadian Socal Insurance Number - Threshold

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

Canadian Social Insurance Number with Additional PII

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

Chinese Identity Card Number

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

Credit Card Information

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

Credit Card Information - Threshold

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

Credit Report

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

Employee Evaluation Information

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

German Social Insurance Number

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

Hong Kong Identity Card Number

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

Indian Permanent Account Number

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

Indonesian Identity Card Number (Nomor Induk Kependudukan)

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

Irish Personal Public Service Number

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

Italian National Identification Number

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

Macau Non-Permanent Resident Identity Card (BIRNP)

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

Macau Permanent Resident Identity Card (BIRP)

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

Malaysian National Registration Identification Card Number

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

Pakistan National Identity Card Number

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

Singapore National Registration Identity Card

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

Social Security Number

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

Social Security Number - Threshold

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

Social Security Number with Additional PII

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

Taiwan Identity Card Number

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

Thailand Population Identification Code

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

UK Drivers License

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

UK Drivers License - Threshold

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

UK Employee Compensation Information

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

UK National Insurance Number

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

UK National Insurance Number - Threshold

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

UK National Insurance Number with Additional PII

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

UK Tax Identification Number

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

UK Tax Identification Number - Threshold

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

Unencrypted Wire Transfer Information

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

US Drivers License

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

US Drivers License - Threshold

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

US Employee Compensation Information

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

US Passport Number

This policy detects US Passport Numbers in various formats.

US Passport Number - Threshold

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

US Taxpayer Identification Number (TIN)

This policy detects US Taxpayer Identification Numbers in various formats.

US Taxpayer Identification Number (TIN) - Threshold

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

Vietnam ID Card Number

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

Security General / Corporate Policies

Audio Files

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

E-mail to Personal Addresses

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

Forwarding Senior Management E-mail or Documents

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

Graphic and Image Files

This policy identifies graphic and image files in various formats.

Large Message or File Size

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

Large Print Job Warning

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

Network Security Threats

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

Password Protection/Encryption: Prohibition

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

Random Sample

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

Sharing of Usernames and Passwords

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

Suspicious E-mail Behavior

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

Transfer of Attachments - Threshold

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

Transfer of Personal E-mail File Folders

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

Video Files

This policy identifies video media files in various formats.

User Defined Policies

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

Common Content

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

Immediate Disqualifiers

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

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

Positive Indicators

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

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

User Defined 1

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

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

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

User Defined 2

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

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

User Defined 3

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

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

Available Actions

The following policy actions are available in the iConsole.

Available Actions: Email

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

Monitor

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

Advise Encryption

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

Encrypt

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

Don't Encrypt

The email is sent unencrypted.

Cancel

The email is not sent.

For emails detected by a CA DataMinder email server agent:

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

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

Enforce Encryption

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

For emails detected by a CA DataMinder email server agent:

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

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

Warn

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

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

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

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

Block

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

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

Global Option

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

Available Actions: Files In Motion

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

Monitor

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

Advise Encryption

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

Encrypt

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

Don't Encrypt

The file is copied onto the removable device unencrypted.

Cancel

The file is not copied.

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

Enforce Encryption

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

Warn

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

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

Block

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

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

Available Actions: Data At Rest

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

Report

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

Replace with Stub File

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

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

Delete

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

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

Global Option

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

iConsole Standard Policies

The iConsole standard policies compromise a predefined set of policies drawn from the CA Foundation Policy Pack (FPP). You can customize these standard policies in the iConsole to quickly roll out CA DataMinder across your organization.

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

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

Who Do the Standard Policies Apply To?

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

More information:

FPP User Groups Created Automatically on the CMS (see page 123)

FPP User Groups Created Automatically on the CMS

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

FPP Base Group

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

FPP Custom Group

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

User Accounts in FPP Custom Group

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

New users

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

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

UnknownInternalSender

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

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

DefaultFileUser

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

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

DefaultClientFileUser

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

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

Editing Policy in the iConsole

You can edit the standard policies in the iConsole.

To edit policies in the iConsole

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

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

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

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

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

3. In the Edit Policy Document page, you can:

   - Edit the Global Options. Double-click the option that you want to edit.
   - Enable or disable triggers for individual policies. Select or clear the relevant checkboxes.
   - Edit the settings for individual policies or triggers. Double-click the policy that you want to edit.

4. Click the Save button in the Edit Policy Document page to save all the changes to the policy document.

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

More information:

Define the Global Options (see page 126)
Enable Policy Triggers (see page 127)
Edit the Policy Settings (see page 128)
Choose a Policy Action (see page 129)
Save the Policy Changes (see page 133)

Define the Global Options

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

To edit the global options

1. In the Edit Policy Document page, expand the Global Options branch.
2. Double-click the option that you want to edit.

   For example, the FPP global options are:

   Action Configuration: Data At Rest

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

   Action Configuration: Data In Motion - Email

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

   Security Officer Contact Information

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

   Miscellaneous: Internal Domains Variable

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

   Miscellaneous: Global Policy Variables

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

Enable Policy Triggers

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

To enable policy triggers

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

   Email

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

   Network

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

   File

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

Edit the Policy Settings

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

To edit policy settings

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

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

   Common Content tab

   Contains settings applicable to all triggers in this policy.

   Many policies include a **Sensitivity** setting:

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

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

   Data In Motion - Email tab

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

   Data In Motion - Network/Endpoint tab

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

   Data At Rest tab

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

   Web - Endpoint tab

   Contains Web trigger settings and policy action for web activity detected by the Internet Explorer endpoint agent.

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

Choose a Policy Action

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

To choose a policy action

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

   Emails

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

   Files In Motion

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

   Data At Rest

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

   Web

   You can block web sites or file uploads, warn the user, or monitor web activity.

   For details about the available actions, see the following sections.

Available Actions: Email

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

Monitor

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

Advise Encryption

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

Encrypt

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

Don't Encrypt

The email is sent unencrypted.

Cancel

The email is not sent.

For emails detected by a CA DataMinder email server agent:

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

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

Enforce Encryption

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

For emails detected by a CA DataMinder email server agent:

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

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

Warn

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

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

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

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

Block

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

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

Global Option

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

Available Actions: Files In Motion

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

Monitor

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

Advise Encryption

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

Encrypt

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

Don't Encrypt

The file is copied onto the removable device unencrypted.

Cancel

The file is not copied.

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

Enforce Encryption

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

Warn

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

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

Block

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

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

Available Actions: Data At Rest

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

Report

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

Replace with Stub File

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

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

Delete

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

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

Global Option

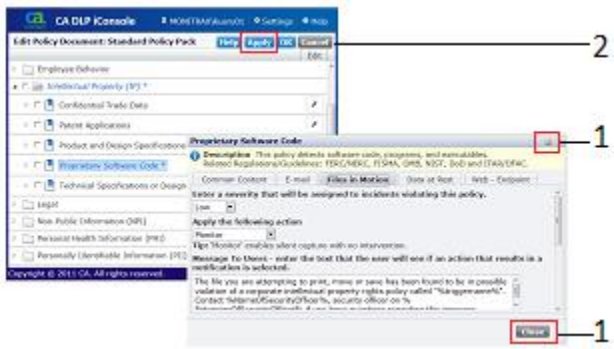
You can also specify a 'Copy File To' location for each of the above actions.

Save the Policy Changes

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

To save policy changes

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



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

   Important! Do not log off without saving your changes.

Policy Tuning

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

More information:

General Tips (see page 134)
Basic Rules (see page 135)
Matching Numbers (see page 136)
Ignore Key Words When They Occur in Disclaimers (see page 137)
Words That Indicate a Definite Non-Match (see page 138)
Threshold Values (see page 139)

General Tips

The main policy customizations are summarized below.

Add words or phrases that, if found, exclude the entire communication

By adding 'excluded' words or phrases to a policy, you effectively create an entire category of communications that cannot cause policy to fire, no matter what other terms or phrases may be present. Use this technique to create exceptions to policy or as a simple way to exclude certain types of company specific communications.

For example, you can permit all communications with the phrase 'Copyright 2011 Your Company, Inc.' to be exempt from policy, without regard to the actual content beyond this phrase. Likewise, you can set a bypass term that allows individuals who know the term to include it in their email, so ensuring that it does not cause policy to fire. For details, see *Words That Indicate a Definite Non-Match*.

Change the number of elements that must be present for the policy to fire.

The minimum number of terms necessary for a policy to fire is known as the 'minscore'.

For many policies, this is a fixed number and cannot be changed. But for policies where it can be changed, such as for the Threshold policies, you can reset it using the minscore(x) function, where x approximates the number of terms that must be present in a document to cause a policy to fire. You must use the Administration console to do this.

In other policies, a Sensitivity setting allows you to influence the number of terms necessary for a policy to fire without needing to know the actual number. A low sensitivity requires fewer terms to be present, placing greater emphasis on not missing violations; a high sensitivity requires more terms to be present, ensuring that the number of false positives is minimized.

Add a template for company-specific data such as account numbers

By adding a template for company-specific material to a policy, you can see a significant reduction in false positives and an overall increase in efficiency. For example, in an Account Number policy, you can add the specific range of account numbers used by your company to ensure that all numbers in that range are detected. If your company uses 10 character account numbers that begin with 'A' followed by 9 digits, you can add this template to the relevant policy field: **%#A\d[9]%**.

Basic Rules

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

Whole words

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

Case

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

Spaces

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

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

Hyphens

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

work-force, **workforce**, **work force**

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

Matching Numbers

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

Syntax

Templates only: %# ... %

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

Separate multiple templates with commas:
`%#<template>%,%#<template>%`

This syntax is not needed for literal matching.

\a or \A

Matches any single letter

\d or \D

Matches any single digit (0-9)

\l or \L

Matches any single letter or digit

\p or \P

Matches any single punctuation character

[M]

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

[M,N]

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

[[a-z]]

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

Examples

867-5309

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

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

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

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

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

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

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

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

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

Ignore Key Words When They Occur in Disclaimers

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

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

Example 1

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

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

Example 2

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

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

Words That Indicate a Definite Non-Match

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

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

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

You typically use Immediate Disqualifier words or phrases to:

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

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

Threshold Values

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

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

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

PII (Personally Identifiable Information)

Account Number - Threshold

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

Credit Card Information - Threshold

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

Social Security Number - Threshold

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

US Individual Taxpayer Identification Number (ITIN) - Threshold

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

PHI (Personal Health Information)

Medical Record Numbers - Threshold

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

NPI (Non-Public Information)

Customer Lists

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

Chapter 10: iConsole Administration

This section is for iConsole administrators only. These are CA DataMinder users with the 'Admin: Manage iConsole' privilege. Privileges are granted to CA DataMinder users in the Administration console.

This section contains the following topics:

Managing Home Pages

Note: You can only create default home pages if you have the 'Admin: Manage iConsole' administrative privilege.

You can create a default home page, available to all users with a specific role. You define the column layout and the portlets included on the default home page. You can also specify whether users are allowed to create personal home pages. (A user creates a personal home page by editing the default home page.)

For example, you can create a set of global portlets but not include them on the default home page. Instead, you allow users to choose which of these portlets they want to include on their personal home page. You can also allow users to create their own portlets.

More information:

Create a Default Home Page

You can create a default home page that is available to all users with a specific role. You can also specify whether users are allowed to personalize this home page by adding or removing portlets, or by creating their own portlets.

About the System Default Home Page

The out-of-the-box default home page for all users is the 'system default' home page, which comprises five global portlets.

The system default home page is assigned to all users who with an Unmanaged role or a Custom role on the Role Assignments page.

Note: Custom roles are assigned automatically to user accounts upgraded from previous versions of CA DataMinder and which were previously assigned to a custom *user category*.

To create a default home page for a specific role

1. Click the Home tab.
2. Click the  Customize link in the top right of the iConsole screen.

   The Customize Home Page dialog displays.
3. Click the Layout tab, and click New Layout.

   The Create New Layout dialog opens.
4. Give the new layout a name. For example, 'HR Reviewers'.

   A message indicates that the layout has been created and is ready for editing.
5. Click the Global Portlets tab.

   The available portlets are displayed.

To arrange the home page

1. Drag portlets and drop them into their desired location in a column.
2. (Optional) Click the  Settings link in a portlet titlebar to configure the portlet.
3. (Optional) Click Collapse Portlet in the titlebar of a portlet to reduce clutter on the screen.

   The home page layout is saved automatically.

To assign a default home page to a role

1. Go to the Administration tab and click Role Assignments.

   The 'Manage Assignments of Resources to User Roles' page appears.

2. Select a role from the User Role list.
3. Go the Settings pane and click Edit.

   The Edit Resources dialog appears for the selected role.

4. Click the Home Page tab.
5. Choose a layout from the 'The Home Page layout that will be used initially' list.
6. Configure additional home page settings for this role. For example, specify whether the home page is optional or not, and whether users are allowed to create personal portlets for inclusion in their home page (and if so, which type of portlets).
7. Click OK.
8. Click away from the Administration tab.

Create a Global Portlet

A *global portlet* can be included on the home page of any user. Global portlets can be optional or mandatory. *A mandatory portlet* does not have a Close button and users cannot remove it from their home page.

To create a global portlet

1. Click the Home tab and select the appropriate layout subtab.
2. Click the  Customize link in the top right of the iConsole screen.

   The Customize Home Page dialog displays.

3. Click the New Portlet tab and select a portlet type.

   The Home Page Portlet Wizard opens.

4. Specify the basic portlet details depending on the portlet type. For example, specify a URL for the RSS Feed Portlet.
5. Select 'Anyone can use this portlet' to make this a global portlet for all users.
6. (Optional) Select 'Pin this portlet to every Home Page' to make this portlet mandatory for all users.

7. Click OK.

   The Assign Roles dialog opens.

8. Select the roles that have access to the new portlet.

   The portlet appears on the home page with default settings.

9. Edit the portlet settings. (see page 29)

Edit a Portlet

Use the Home Page Portlet Wizard to edit portlet settings.

Note: Click the question mark in the portlet title bar to get details about the portlet.

To edit a portlet

1. Click  Settings in the portlet title bar.
2. Click the  Portlet Definition button to launch the Home Page Portlet Wizard.
3. Specify the portlet settings.
4. Click Finish to close the wizard.

Role Assignments

Note: You can manage user roles in the iConsole if you have the 'Admin: Manage iConsole' administrative privilege.

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 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.

More information:

Which Features Can Be Assigned To User Roles? (see page 145)
Set Up Role Assignments (see page 150)

Which Features Can Be Assigned To User Roles?

You assign settings, portals, searches and reports to individual user roles in the Role Assignments page of the Administration tab:

Settings

Specify the default settings for each user role. You can also optionally enforce individual settings to prevent users from modifying them.

Available settings are organized into these groups:

- Audit (see page 23)
- BusinessObjects (see page 25)
- General (see page 148)
- Home page (see page 148)
- Printing (see page 23)
- Search (see page 24)

Types of portlets that can be created

Specify which portlets users can create and add to their home page.

The portlet types that you select are added to the New Portlet tab in the Customize dialog. The New Portlet tab lists the portlet types available to users who want to add a personal portlet to their home page.

Note: This element is only visible if the role that you are editing has 'Allow portlet creation' enabled. You can allow or disallow portlet creation for all users under Home Page, Settings.

Portlets that are ready to be used on the Home Page

Specify which global portlets users can add to their home page.

The global portlets that you select are added to the Global Portlet tab in the Customize dialog. The Global Portlet tab lists all existing global portlets that users can add to their home page.

Available Search and Reports

Specify which searches and reports are available to users with the current role. These searches and reports are listed on the Review tab.

More information:

Audit Settings (see page 146)
BusinessObjects Settings (see page 147)
General Settings (see page 148)
Home Page Settings (see page 148)
Printing Settings (see page 149)
Search Settings (see page 149)

Audit Settings

These settings control audit behavior in the Search Results screen.

Move to Next Event After Auditing

Specifies whether focus moves automatically to the next event after an event has been reviewed or audited.

Remove Events After Auditing

Specifies an event is removed from the Search Results after it has been reviewed or audited.

Scroll Past Headers in Email Pane

Specifies whether the display scrolls automatically past the recipient and subject details to the body text when reviewing an individual email event.

Show Incidents / Show Issues / Show Event History

Specifies whether incident details, audit issues and the event history are displayed in the right-hand pane when reviewing an individual event.

Note: CA DataMinder generates an *incident* each time a policy trigger fires.

Incidents Display / Issues Display / Event History Display

(Applicable only if the corresponding 'Show' check box is selected.) Specifies the initial level of shown in the right-hand pane when reviewing an individual

BusinessObjects Settings

These settings control which BusinessObjects features are available in the iConsole. For example, you can choose whether to show BusinessObjects reports in the Review tab. You can also specify the report format (HTML or PDF) and the folder where the reports are saved in InfoView.

Use BOE Integration

Allows you to run BusinessObjects reports for CA DataMinder.

Default Format for BOE Reports

Specifies the output format for CA DataMinder BusinessObjects reports. The supported formats are PDF and HTML.

Allow BOE Portlets

Allows you to add BusinessObject report portlets to your home page.

Allow BOE Reports

Adds BusinessObjects reports for CA DataMinder to the BusinessObjects page of the iConsole Review tab.

Show a Link to InfoView

Adds an InfoView link to the BusinessObjects page of the iConsole Review tab.

Show Personal Reports

Adds your customized BusinessObjects reports to the BusinessObjects page of the iConsole Review tab.

Personal Reports Folder

Specifies the folder where your customized BusinessObjects reports for CA DataMinder are found.

Your customized BusinessObjects reports for CA DataMinder are available in InfoView on the Document List page. Specify the folder on the Document List page that contains your customized BusinessObjects reports.

General Settings

These settings configure the default behavior for iConsole home pages.

High Visibility

Specifies whether you want to display the home page with a larger, more easily readable font.

Remote Access

(Applies only if you connect to the iConsole using Remote Desktop Connection)

Optimizes the iConsole display for RDC connections. In particular, this setting turns off graphics features such as background animations in iConsole dialogs. Such graphics can affect iConsole performance during RDC sessions.

Home Page Settings

These settings control home page layout and behavior for the selected role.

Allow Portlet Auto Refresh

Enables or disables automatic updates for report portlets.

Report portlets normally get refreshed at regular intervals (every five minutes, by default). Such updates can adversely affect iConsole performance. refresh after a time period. Clear this check box to prevent report portlets from bing refreshed during the current session.

Allow Portlet Creation

Allows users to add personal portlets to their home page.

Show Home Page

Specifies whether a home page is displayed when you log into the iConsole.

The home page layout that will be used initially

Specifies the default home page layout for the current role. Users assigned to this role see this layout when they use the iConsole for the first time.

Printing Settings

These settings determine whether printed search results include the event text content, summary details, and extended information.

Print Content

Prints the text content of captured events (if available).

Print Event Summary

Prints the event metadata. This includes details about any triggers that fired plus an indication of why they fired.

The metadata also includes details such as the event type, participants, timestamp, and event source.

Print Audit Summary

Prints any audit details associated with the event, including audit histories for individual audit issues.

Search Settings

These settings control how search results are displayed.

Search Results Page Size

Specify the maximum number of results per page.

Multi-line Row

Specify whether details for individual events can wrap over multiple lines of text.

Show results in bold until viewed

Specify whether events are shown in bold in the results screen if you have not viewed them yet. After you view an event, it is shown in normal text.

Content Server

If your iConsole supports content searches, you can specify which content proxy server to use.

The content proxy server links the console to a content database. You may prefer to manually select a content proxy server you have:

- Multiple proxy servers connected to different content databases. Choose the proxy server that is connected to the database containing the captured data you want.
- Multiple proxy servers connected to a single content database. Choose the proxy server with, for example, the fastest or the most secure database connection.

Set Up Role Assignments

You assign settings, portals, searches and reports to individual user roles in the Administration tab.

Follow these steps:

1. Log on to the iConsole using a CA DataMinder account with the 'Admin: Manage iConsole' privilege.
2. Go to the Administration tab and click Role Assignments.

   The 'Manage Assignments of Resources to User Roles' page appears.
3. Go to the User Role list.

   Select a role from the list. If the role you want is not listed, click Add.
4. Assign settings, portals, searches and reports to the role.

   a. Go to the required pane and click Edit.

   b. Select the features (see page 145) you want.

   Note: When you assign default settings to the role, you can enforce individual settings to prevent users from modifying them.
5. Click away from the Administration tab.

   The new role assignments are saved automatically.

More information:

Which Features Can Be Assigned To User Roles? (see page 145)

User Administration

Note: You can only manage CA DataMinder user accounts in the iConsole if you have the 'Admin: Manage iConsole' administrative privilege.

You can use the iConsole to update account details for CA DataMinder users. You can also create new user accounts.

More information:

Manage User Account Details (see page 151)
Create New User Accounts (see page 152)
User Roles (see page 153)
Security Models (see page 155)
Policy Roles (see page 158)
Management Groups (see page 159)
Exempt Users (see page 160)

Manage User Account Details

You can use the iConsole to update account details for CA DataMinder users. For example, you can assign users to a new role or change their security model.

To manage user accounts

1. Log on to the iConsole using a CA DataMinder account with the 'Admin: Manage iConsole' privilege.
2. Go to the Administration tab and click Users.
3. Search for the users you want. You can search by user name or group. You can also search for users with a specific role.
   a. Enter the user, group, and role details. You do not need to enter the full name of the user or group.
   b. Click Search.

   The search results show all matching user accounts.

   Note: Double-click a user to view their email addresses and group history.
4. Select the check box for each user account that you want to edit.
5. Update the account details for the selected users. For example, you can:
   - Move these users into a new group.
   - Delete these user accounts.
   - Set the security model for these users.
   - Set the user role.
   - Set the exemption status. For example, you can exempt users from policy.

Create New User Accounts

In a typical CA DataMinder deployment, user accounts are created automatically when a user logs onto a computer hosting a CA DataMinder endpoint agent. Or an administrator uses the Account Import feature to synchronize CA DataMinder user accounts with your principal user directory (such as Microsoft Active Directory.)

But the iConsole also enables you to create new user accounts. For example, this is useful if you want to create additional Administrator or Reviewer accounts that are not linked to actual users in your organization.

To create new user accounts

1. Log on to the iConsole using a CA DataMinder account with the 'Admin: Manage iConsole' privilege.
2. Go to the Administration tab and click Users.
3. Click Create User.
4. Enter the required details in the Create User dialog, including:

   Role

   Choose a role for the new user account. T

   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.

   Security Model

   Assign a security model to the new user.

   The security model determines which events a user is permitted to see when they run a search in the iConsole or Data Management console. (In technical terms, it controls access to events stored in the CMS database.)

   Policy Role

   If the new user is assigned to a policy-based security model, you must also assign 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.

   Management Groups

   If the new user is assigned to a management group-based security model, you must also assign a management group.

   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.

Exempt from policy

Click this check box to exempt a user 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.

More information:

Management Groups (see page 159)
Policy Roles (see page 158)
User Roles (see page 153)
Security Models (see page 155)

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 154)

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 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.

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 158) 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.

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.

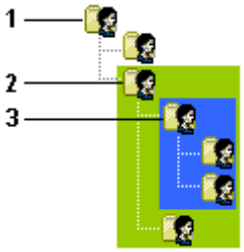
A *policy role* links a user to a collection of policy classes. In effect, the policy role determines which policy classes a user is permitted to see. When the user runs a search, the results only include events associated with these policy classes.

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.

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.

Managing Searches, Reports, and Dashboards

You can manage searches, reports and dashboards in the iConsole. You can only manage searches, reports, or dashboards globally if you have the 'Admin: Manage iConsole' administrative privilege.

Specifically, you can:

- **Install a new search (see page 163):** You can install a completely new search based on your own customized XML search definition file. This is the most flexible method. When published, the new search is available to all users.
- **Customize a Search (see page 33):** Any iConsole user can customize a search (no administrative privilege is needed), but the new search is only available to that user.
- **Derive a new search (see page 164):** A derived search is similar to a customized search but unlike normal customized searches, it can be published and made available to users. It is also possible to edit the XML definition file of a derived search.
- **Export a search (see page 165):** You can export a search definition as XML, modify properties, and re-install it. This way you can customize properties that you cannot edit directly in the iConsole.
- **Test a search (see page 166):** Before you make a new search available to your users, you need to validate its definition file against the corresponding stored procedure in the CMS database.
- **Publish or unpublish a search (see page 167):** To make a new search available to all other iConsole users, you need to publish it. Likewise, to remove a search so it is no longer available, you must unpublish it.

More information:

How to Install a New Search (see page 163)
Derive a New Search (see page 164)
Export a Search as XML (see page 165)
Test a search (see page 166)
Publish or Unpublish a Search (see page 167)
Stored procedure (SP) files (see page 167)
Search definition (XML) files (see page 168)
Customize a Search (see page 33)

How to Install a New Search

There are several ways of adding new searches to the iConsole. For example, you can customize an existing search or derive a new search from an existing search. This section describes how to install a completely new search.

Follow these steps:

1. Install an XML search definition file onto the CMS.

   This file defines the search parameters and the layout of the search results screen. It also references a stored procedure (SP) in the CMS database.

2. Test the new search.

   You need to confirm that the search correctly references the SP and returns a valid set of search results.

3. Publish the new search.

   When you publish a new search, it becomes available to all other iConsole users and is added to the Searches list.

More information:

Stored procedure (SP) files (see page 167)
Search definition (XML) files (see page 168)

Install a Search

To add a new search, you must first install an XML search definition file onto the CMS.

To install a search

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.

2. Click the Install link.

   Find this link at the top left of the screen.

3. In the Install Search dialog:

   a. Click Browse to locate the XML search definition file you want to install.

   b. Select or clear the 'Publish after install?' check box.

      If you select the check box, the search is published and made available to all other iConsole users as soon as it is installed.

      If you clear this check box, the search is not published yet.

   c. Click the Install button.

Uninstall a Search

To delete a search from the CMS, you need to uninstall the search.

To uninstall a search

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.

2. Click the check box for the search you want to delete.

3. Click the Actions, Uninstall.

   The search is deleted from the CMS.

More information:

Stored procedure (SP) files (see page 167)
Search definition (XML) files (see page 168)
Test a search (see page 166)
Publish or Unpublish a Search (see page 167)

Derive a New Search

A derived search is similar to a customized search in that both are variations of an existing search. But unlike normal customized searches, derived searches can be published and made available to users.

It is also possible to edit the XML definition file of a derived search, allowing you to change text labels and default parameter values. In addition, unlike normal customized searches, a derived search can be based on an unpublished existing search. This is useful, for example, if you want users to use a modified version of the default iConsole Standard Search but without the 'real' Standard Search being available to them. For full implementation details, see the *iConsole Search Definition Guide*; search for 'derived searches'.

To derive a new search from an existing search

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.

2. Click the check box for the search you want to use as the start point.

3. Click Actions, Edit Properties

   The Properties dialog appears.

4. Specify the search properties for the new search.

   For example, choose which columns to show in the results screen. You can also click Customize to hide or unhide available search parameters.

5. Click Save to save the customized search.

6. In the Save Search dialog, enter a name and description for the modified search.

7. Export and edit the underlying XML search definition (see page 165).

More information:

Test a search (see page 166)
Publish or Unpublish a Search (see page 167)
Export a Search as XML (see page 165)

Export a Search as XML

Not all search modifications can be made directly in the iConsole. If you want to change the text labels for search parameters or amend other parameter attributes, export the search and edit the underlying XML in the new definition file.

To edit the XML search definition:

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.

2. Click the check box for the search you want to export.

3. Click Actions, Export.

4. Use an XML editor to modify the exported XML file.

To re-install the modified XML search definition file:

1. Return to the Administration, Manage Stored Searches screen.
2. Click the Actions link *at the top left of the screen*.

   The Install Searches dialog opens.
3. Specify the modified XML file in the Install Searches dialog.

   The new derived search, including the latest XML modifications, is added to the Searches folder.
4. Test the new search to confirm that it returns results as expected.
5. Publish the new search.

   When you publish a new search, it becomes available to all other iConsole users and is listed in the Review tab.

Test a search

The parameters in a search definition file must be validated against the corresponding stored procedure in the CMS database.

You can only test a search if it is unpublished.

To test a search

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.
2. Click the check box for the search you want to test.
3. Click Actions, Edit Properties to amend the default search parameters.

   The Properties dialog opens.
4. Save your changes and close the Properties dialog.
5. Click Actions, Test to run the search.

Publish or Unpublish a Search

To make a search available to all other iConsole users, you need to publish it. To remove a search so it is no longer available to other users, you must unpublish it. The Manage Stored Searches screen indicates which searches are already published.

Note: If you unpublish a search that has a customized search associated with it, the iConsole displays an error when a reviewer attempts to run this customized search.

To publish or unpublish an individual search

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.
2. Click the check box for the search you want.
3. Click the Actions button.
4. Click Publish or Unpublish, as required.

To publish or unpublish multiple searches

1. Go to the Administration tab and click Searches.

   The Manage Stored Searches screen appears.
2. Click the check boxes for the searches you want.
3. Click the Actions link *at the top left of the screen*.
4. Click Publish Selected Searches or Unpublish Selected Searches, as required.

Stored procedure (SP) files

A search SP contains SQL statements that define a specific search for captured or imported events. The iConsole supports search SPs for both SQL Server and Oracle databases. Each XML search definition file references the name of the search SP.

The name of the stored procedure file is referenced in the search definition file.

Any search parameters specified in the stored procedure are hard coded and cannot subsequently be changed by administrators when they write the XML search definition, or customize the search in the iConsole. For example, you may want to fix the names of check boxes, or the available items in a list box.

For details about search SP syntax and naming requirements, please see the *iConsole Search Definition Guide*.

More information:

Search definition (XML) files (see page 168)

Search definition (XML) files

The screen layouts for an individual iConsole search are defined by parameters in a search definition file. Search definition files are written in XML and must contain the following parameters:

- The name of the search stored procedure (SP) that will perform the actual search query. For example:

  ```
  spname="PUB_WGN_7DAY_EMAIL_RESEARCH"
  ```

- The name and description of the search definition
  label="Research Department Weekly E-mails"

  ```
  description="E-mails sent by research department in last 7 days"
  ```

- The format of the Search Properties screen, for example, the available check boxes and list boxes and how they are grouped.

  ```
  <parameter name="chkWE" type="checkbox"
  argpos="1" label="Email Events:"
  value="false" align="right"
  tooltip="Select to get captured Email Events"/>
  ```

- The layout of the Search Results screen, for example, the number of columns and their label names.

  ```
  <results>
  <column name="EmailCount" label="The number of emails stored is:" type="numeric"
  width="50%" style="color:red"/>
  </results>
  ```

  Note: In the extracts above, the command syntax has been spread over multiple lines for readability purposes. However, the actual command must be on a single line in the batch file.

  Note: An individual search definition file can contain default parameters to define the layout of multiple search definitions.

For more details, see the *iConsole Search Definition Guide*.

More information:

Stored procedure (SP) files (see page 167)

Integration with BusinessObjects Enterprise

The BOE Integration component enables the iConsole to log on to BusinessObjects Enterprise and retrieve available BusinessObjects reports for CA DataMinder.

To configure the BOE Integration component

1. Log on to the iConsole using a CA DataMinder account with the 'Admin: Manage iConsole' privilege.
2. Go to the Administration tab and click BusinessObjects.
3. Specify the integration settings (see page 170) in the BusinessObjects page:

More information:

BusinessObjects Integration Settings (see page 170)

BusinessObjects Integration Settings

Specify the following integration settings:

The name or IP address of the server hosting BusinessObjects.

Specify the FQDN (fully qualified domain name) or IP address of the server hosting BusinessObjects Enterprise.

The TCP port used by the iConsole to log on to BusinessObjects Enterprise.

In BusinessObjects terminology, this is the CMS Name Server Port. It defaults to port 6400. Normally, you do not need to change this port number. But if your BusinessObjects Enterprise installation uses a different port number, specify that number here.

The TCP port to be used by the iConsole to connect to the BusinessObjects web service.

The iConsole calls this web service to display the available BusinessObjects reports, retrieve report results, and access the InfoView web portal.

The default is port 8080. Normally, you do not need to change this port number. But if the BusinessObjects Enterprise web service uses a different port number, specify that number here.

The InfoView folder containing CA DataMinder reports.

Specifies the folder where common BusinessObjects reports for CA DataMinder are found.

BusinessObjects reports for CA DataMinder are available in InfoView on the Document List page. Specify the folder on the Document List page that contains the common reports. (Users can save their own customized reports in a separate 'Personal Reports' folder.)

Enable integration with BusinessObjects Enterprise?

Select this check box to enable users to run BusinessObjects reports for CA DataMinder.

Note: Any changes to these settings apply to *all* your iConsole front-end web servers.

Appendix A: Reference (iConsole)

This chapter covers reference information for iConsole users and administrators.

This section contains the following topics:

About Single Sign-On

If single sign-on (or 'SSO') is enabled for the parent CMS of the application server, users skip the logon dialog when they start up the iConsole. 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.

(To log on using a different account, a user must first log out of the iConsole, then log back on from the Logon screen.)

To configure CA DataMinder to use single sign-on, you must edit the CMS machine policy. You can also grant the administrate privilege Admin: Use single sign-on to individual users (this overrides the CMS policy). Note that account names for CA DataMinder users must be the same as their native Windows user name (sometimes referred to as the user logon name). That is, an account name prefixed with the user's domain, for example, unipraxis\lsteel.

For full details, see the Administration console online help; search for 'single sign-on'.

iConsole Bookmarks

Single Sign-on must be enabled for iConsole search bookmarks to work as intended. If you bookmark a search, it is added to your Favorites in Internet Explorer. Normally, when you click the search shortcut in the Favorites list, the iConsole takes you directly to the Search Results page or Customize Search page. But if Single Sign-on is not enabled, it takes you instead to the Logon page (see page 15).

Appendix B: 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