CA DataMinder

Release Notes

Release 14.6

CA Technologies Product References

This document references the following CA Technologies products:

- CA DataMinder™
- CA Business Intelligence™

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: What Is CA DataMinder?

CA DataMinder provides real time risk management of internet communications, right across the organization. Specifically, CA DataMinder enables organizations to capture and control targeted e-mail, file, IM and web activity. CA DataMinder can also monitor usage of other applications.

This section contains the following topics:

Chapter 2: What is in the CA DataMinder Image?

This CA DataMinder image contains all the software you need to deploy CA DataMinder, including CA DataMinder FastStart. It includes product software for installing CA DataMinder on servers and client machines. It contains:

setup.exe and setup32.exe

Located in the root of the distribution image, these executables provide a single starting point for all (manual) installation or upgrade operations, including CA DataMinder FastStart. They launch a universal installation wizard that guides users through the deployment process and launches the relevant component wizard (linked to component source images in the Windows folder; see below).

Run setup.exe on systems with 64-bit operating systems.

Run setup32.exe on systems with 32-bit operating systems.

\3rd_Party folder

Contains the readme for DataDirect Connect for JDBC, a third party component embedded in the CA DataMinder infrastructure.

\BusinessObjects folder

Contains files needed for integration with BusinessObjects Enterprise, including files required by the BusinessObjects Universe for CA DataMinder and BusinessObjects reports for CA DataMinder.

\Linux folder

Contains the software for installing CA DataMinder on Linux machines.

The \WgnMilter subfolder contains install.sh for installing the Milter MTA agent. This agent enables CA DataMinder to integrate with Sendmail and Postfix.

\Redist folder

Contains third party components redistributed with CA DataMinder, including SQL Server 2012 Express Edition and the BusinessObjects .NET SDK Runtime.

Note: CA Business Intelligence is not included in the CA DataMinder distribution image. Instead, CA Business Intelligence is available for download on the CA Support site, under "CA DataMinder Suite" product downloads.

\Support folder

Contains support utilities such as wgncheck.exe and scripts to generate installation transforms (these enable you to apply customized configuration changes to Windows Installer packages).

\Windows folder

Contains all the CA DataMinder installation source images, such as server.msi and integration.msi.

These source images are invoked by setup.exe. They contain the software for installing the various CA DataMinder components.

Chapter 3: Requirements

Hardware and software requirements for CA DataMinder components are listed in the 'Requirements' chapter of the *Platform Deployment Guide*.

Requirements for specific CA DataMinder components, such as archive integration agents or the File Scanning Agent, are also included in the appropriate guides.

Chapter 4: Documentation

CA DataMinder documentation is available to view or download from CA Support Online: http://ca.com/support

About the Bookshelf

The Bookshelf provides access to all CA DataMinder documentation from a central location. The Bookshelf includes the following:

- Single expandable list of contents for all guides in HTML format
- Full text search across all guides with search terms highlighted in the content and ranked search results

  Note: When searching for purely numeric terms, precede the search value with an asterisk.
- Breadcrumbs that link you to higher level topics
- Single index across all guides
- Links to PDF versions of guides for printing

CA product documentation bookshelves are available for download in ZIP files titled 'All Guides Including a Searchable Index'.

To access the CA DataMinder bookshelf

1. Go to Search Documentation on the CA Support Online site.
2. Type CA DataMinder for the product, select a release and language, and click Go.
3. Download the ZIP file to your desktop or other location.
4. Open the zip file and drag the bookshelf folder to your desktop or extract it to another location.
5. Open the bookshelf folder.
6. Open bookshelf.html.

   The bookshelf opens.

Chapter 5: Announcements

This section contains the following topics:

Announcements for 14.6

This section highlights important announcements for the CA DataMinder 14.6 release.

Announcements:

IBM Content Collector Certification

CA DataMinder 14.6 includes certification for IBM Content Collector (ICC) 3.0 and 4.0.

Microsoft Exchange Server 2013 CU3 Certification

The Exchange Server agent can analyze and apply policy to emails passing through Microsoft Exchange Server 2013. Microsoft Exchange Server 2013 now requires MAPI connectivity using **RPC over HTTP(S)**.

Note: For full deployment details, see the Exchange, Domino, and IIS SMTP Integration chapter in the *Message Server Integration Guide*.

Certified CA DataMinder components

The following CA DataMinder components have been certified with this release.

- Outlook Agent
- Exchange Server Agent (ESA)
- iConsole
- Event Import
- WgnCred
- WgnCheck

Limitations

Microsoft has made significant architectural changes related to Outlook MAPI. To support the new architecture, CA DataMinder requires adjustments in the File Scanning Agent, Quarantine Manager, and Universal Adapter. These updates are planned for the next release of CA DataMinder. The following limitations are still in place:

FSA scans of Exchange Public Folders

The FSA cannot scan items in Public Folders on Exchange 2013 servers.

This limitation is caused by changes in Exchange 2013 support for MAPI.

Quarantine Manager

The Quarantine Manager is *not* supported on Exchange 2013 servers. Specifically, the Quarantine Manager is unable to release quarantined emails from mailboxes on Exchange 2013 servers. This limitation is caused by changes in Exchange 2013 support for MAPI.

If you want to use the CA DataMinder quarantine feature, configure the Quarantine Manager to use a mailbox on an Exchange 2007 or 2010 server. (The Quarantine Manager uses this mailbox to send emails released from quarantine on to their intended recipient. For full details, see the Quarantine Manager chapter in the *Platform Deployment Guide*.)

Universal Adapter

The Universal Adapter (UA) unable to import emails from journal mailboxes Exchange 2013 servers.

This limitation is caused by changes in Exchange 2013 support for MAPI.

(The UA is typically deployed used to pre-process emails before they are stored in an email archive system.)

More information:

Support for Microsoft Exchange Server 2013 (see page 38)

Announcements for 14.5

This section lists important changes in CA DataMinder 14.5.

Announcements:

Limitations in Support for Microsoft Exchange Server 2013

The Exchange server agent can now analyze and apply policy to emails passing through Microsoft Exchange Server 2013. For full details, see the Exchange, Domino, and IIS SMTP Integration chapter in the *Message Server Integration Guide*.

Support for Exchange 2013 in the first CA DataMinder 14.5 release had several limitations. These limitations were caused by a known issue plus various internal changes in Exchange 2013. These limitations have been fixed in a Release 14.5 hotfix (see page 54).

The limitations were as follows:

Outlook endpoint agent

If an Outlook client is connected to Exchange 2013, the CA DataMinder Outlook endpoint agent can successfully apply policy to incoming and outgoing emails. But note the following limitations:

- The Outlook endpoint agent captures duplicate versions of any email attachments.

  That is, the agent captures two copies of each attachment. However, policy is correctly applied to any attachments. For example, classifier triggers can successfully classify attachments and apply control actions (such as blockings or warnings) where necessary.

- The Outlook endpoint agent cannot capture RMS-restricted emails.

  (Microsoft Windows Rights Management Services (RMS) technology is typically used to restrict how employees use corporate emails, Word documents, and Web pages.)

Note: These agent limitations are caused by a known issue in Exchange Server 2013. However, this known issue has been fixed in the forthcoming Cumulative Update (CU2) release of Exchange Server 2013. If your Outlook clients connect to Exchange 2013 CU2, the Outlook endpoint agent does not suffer from these limitations. (We expect CU2 for Exchange Server 2013 to be released in Spring 2013.)

Event Import

Event Import is unable to import emails from journal mailboxes on Exchange 2013 servers.

This limitation is caused by changes in Exchange 2013 support for MAPI.

The following limitations remain:

FSA scans of Exchange Public Folders

The FSA cannot scan items in Public Folders on Exchange 2013 servers.

This limitation is caused by changes in Exchange 2013 support for MAPI.

Quarantine Manager

The Quarantine Manager is *not* supported on Exchange 2013 servers. Specifically, the Quarantine Manager is unable to release quarantined emails from mailboxes on Exchange 2013 servers. This limitation is caused by changes in Exchange 2013 support for MAPI.

If you want to use the CA DataMinder quarantine feature, configure the Quarantine Manager to use a mailbox on an Exchange 2007 or 2010 server. (The Quarantine Manager uses this mailbox to send emails released from quarantine on to their intended recipient. For full details, see the Quarantine Manager chapter in the *Platform Deployment Guide*.)

Universal Adapter

The Universal Adapter (UA) unable to import emails from journal mailboxes Exchange 2013 servers.

This limitation is caused by changes in Exchange 2013 support for MAPI.

(The UA is typically deployed used to pre-process emails before they are stored in an email archive system.)

License File No Longer Required

Although the Tools menu in the Administration console includes an option to install a license file, you do not need to install a license file to be able to use and deploy CA DataMinder 14.5. Clean installs and upgrades will be fully functional, without time limits or user limits. You do not need to reinstall the license after you upgrade existing installations.

Note: Handling of custom User System Master Policy files remains unchanged. If you are using USMP files issued by CA Technologies Support to extend the policy schema, you must still reinstall these files after upgrades.

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

Internet Explorer Agent is Superseded by Client Network Agent

CA DataMinder no longer supports an Internet Explorer endpoint agent. Instead, you can use the Client Network Agent (or 'network agent') to control web activity on endpoint computers.

The Internet Explorer agent could only apply policy to web activity in Internet Explorer browsers. Conversely, the network agent can apply policy to network activity in any browser.

Note: The Internet Explorer agent applied Web triggers to web activity. By comparison, the network agent applies Data In Motion triggers.

Replacing Web Triggers After Upgrading CA DataMinder

If you previously used the Internet Explorer agent to control Internet activity, you must deploy the network agent and set up new Data In Motion triggers to replace your old Web triggers. For details, see the *Upgrade Guide*.

More information:

Client Network Agent (see page 42)

Adobe Flash No Longer Used in iConsole

The iConsole homepage now uses Sencha Ext JS to create charts. In previous releases, the iConsole used Adobe Flash.

We have made this change to reflect emerging industry trends and the potential discontinuation of Adobe Flash.

FaceTime Renamed to Actiance

FaceTime Communications changed its name to Actiance. There are no changes in CA DataMinder's support of the Actiance IM format or configuration parameters.

SQL Server 2012 Express Edition Included with CA DataMinder

In release 14.5, the \Redist folder in the CA DataMinder image includes SQL Server 2012 Express Edition. In previous releases, the CA DataMinder image included SQL Server 2008 R2 Express Edition.

Features No Longer Supported

The following features are no longer supported in the current version of CA DataMinder:

IE Agent

CA DataMinder no longer supports an Internet Explorer endpoint agent (see page 22).

EMC EmailXtender Integration

CA DataMinder no longer supports integration with EmailXtender. Specifically, the External Agent API no longer integrates with EmailXtender 4.8 SP1 Build 263.

Copy and Paste for Policy List Items

The Administration Console no longer lets you copy list items from the policy editor to an external application. This change is a result of an enhancement that allows the copying of trigger settings between triggers in different policies.

Exporting the User Hierarchy to Spreadsheets

The Administration Console no longer lets you export the user hierarchy to spreadsheet-compatible .CSV files. Specifically, the Export Hierarchy to File dialog no longer includes a 'Spreadsheet Data File' export option. This feature has been dropped due to limitations in the export format .

However, the Administration console still supports user hierarchy export to XML files and command files.

Announcements for 14.1

This section lists important changes in CA DataMinder 14.1.

Announcements:

CA DLP is Now CA DataMinder

CA Technologies is renaming its security portfolio to follow the *Minder* product family.

Consequently, CA DLP has been renamed to CA DataMinder in the current release. This name change highlights the cohesion between CA DataMinder and other CA Security products, especially the integration between CA SiteMinder® and the CA DataMinder Content Classification Service.

Changes to User Roles

This release includes a number of changes affecting user roles (previously called user categories).

User Categories Now Called User Roles

There is an important terminology change in the current CA DataMinder release.

Specifically, the term *User Category* has been replaced by *User Role*. The default user roles are the same as the old user categories (for example, Manager, Reviewer, Policy Administrator, and User). When you assign a user to a User Role, the user inherits the default administrative privileges and security model assigned to that user role.

Cannot Create 'Custom' User Roles

In previous releases, the administrative privileges assigned to an individual user derived from that user's User Category (such as Manager or Reviewer). However, it was also possible to assign a custom set of administrative privileges to an individual user. Such users were automatically assigned to a 'Custom' user category.

In the current version of CA DataMinder, you cannot directly change a user's privileges. As a result, it is no longer possible to create a 'Custom' user role. Instead, you can only change a user's privileges by reassigning the user to a different user role. This change has been introduced to support role-based iConsole configuration (see page 47). Briefly, you can now specify which iConsole features (portlets, searches, and so on) are available to users with specific user roles.

If you upgrade from a previous version of CA DataMinder, any existing user assigned to a custom role retains this custom role in the current version of CA DataMinder. However, such custom user roles are not supported in the iConsole. In particular, you cannot specify which features are available to users with custom roles when they use the iConsole. In this situation, we recommend that you assign users without a recognized role to an equivalent 'official' user role. Do one of the following:

- Manually reassign users with a custom role to one of the default user roles.
- Add new user roles that correspond to the various custom roles held by your users. Then reassign these users to the new user roles. CA DataMinder provides a 'CustomRoleUpgrade' utility that automates this process.

  For instructions, search for 'CustomRoleUtility' in the *Upgrade Guide*.

Note: This move away from custom user roles also affects the CA DataMinder Primary Administrator (see the next section).

Primary Administrator Account Is No Longer Unique

When you install a CMS, you must specify an administrator account. In previous releases, this account was the Primary Administrator, which had a 'Custom' user role. This account had full administrative privileges. These privileges could never be changed and the account could never be deleted.

In the current CA DataMinder release, the Primary Administrator no longer has a unique role but is instead assigned to the Administrator role. All user accounts assigned to the Administrator role have equal administrative authority. All have the full set of privileges, and no privilege can be withdrawn from the Administrator role or from individual administrators. In addition, any administrator can now:

- Reassign an administrator's role to a role with fewer privileges (such as a Manager).
- Delete any other administrator account.

These changes apply equally to the Primary Administrator account that you created when you installed the CMS. They also apply to your existing Primary Administrator account if you upgrade from an earlier version of CA DataMinder. For example, any CA DataMinder administrator can now delete or reassign your Primary Administrator.

Note: This role change for the Primary Administrator change has been introduced to support role-based iConsole configuration (see page 47). Briefly, you can now specify which iConsole features (portlets, searches, and so on) are available to users with specific user roles.

No Network Agent in 14.1

There is no 14.1 version of the Network agent (also known as the Network Boundary Agent or NBA). However, r12.5 and 14.0 versions of the Network agent are supported for use with CA DataMinder 14.1.

Likewise, the *Network Implementation Guide* has been omitted from the CA DataMinder 14.1 bookshelf.

Apply the BusinessObjects 3.1 SP4 Patch

(Applicable only if you want to run BusinessObjects reports for CA DataMinder)

In CA DataMinder 14.0, integration with BusinessObjects Enterprise was provided through CA Business Intelligence 3.2. This version of CA Business Intelligence includes SAP BusinessObjects Enterprise XI 3.1 SP3, a suite of information management, reporting, and query and analysis tools.

However, the current version of CA DataMinder requires BusinessObjects Enterprise XI 3.1 SP4. Therefore, you must install the SP4 patch after you upgrade CA DataMinder. The patch file is cabi-windows-boeXIR3_SP4.zip. It is available here:
`ftp://ftp.ca.com/CAproducts/CABI/CABI-3.x/boeXIR3_SP4/Windows`

Contact CA Technical Support if you cannot access this location.

For full SP4 installation instructions, see the 'Installing CA Business Intelligence section of the *Reports Integration Guide*.

Performance Counters Now Supported in 64-bit Perfmon.exe

On 64-bit systems, all CA DataMinder performance counters are now supported in the default 64-bit version of the Performance applet (perfmon.exe).

Previously on 64-bit systems, most CA DataMinder performance counters were only supported in a 32-bit version of the Performance applet. This anomaly particularly affected performance counters for the policy engine hub when the hub was installed on a 64-bit Exchange 2007 or 2010 server.

If you previously used the 32-bit Performance applet to monitor CA DataMinder components on a 64-bit system, you must switch to the 64-bit Performance applet after upgrading to CA DataMinder 14.1.

Background

On a 64-bit Windows operating system, there are two versions of perfmon.exe:

- A 64-bit version is available in the \Windows\System32 folder. This is the main System folder for the 64-bit operating system.

  Why 'System32'? The folder name, an apparent misnomer, is a legacy of the folder naming scheme in earlier Windows operating systems.

- A 32-bit version is available in the \Windows\SysWOW64 folder.

  Why ‘WOW64’? On a 64-bit Windows operating system, there is an emulation of a 32-bit operating system called ‘Windows on Windows 64’, or WOW64.

Change in Email Address Variable Substitution Format

The substitution format of some variables in user notifications and email replies have changed: The exact format of the email address replacement string depends on the type of email address. For SMTP mail it is for example "Spencer Rimmel(spencerrimmel@unipraxis.com)" and for Exchange mail "Spencer Rimmel(spencer rimmel(unipraxis))". This applies to the %address%, %to%, %from%, %cc%, and %bcc% variables.

For more details, see the *User Notifications* chapter in the CA DataMinder *Policy Guide*.

Initial Data Warehousing Job Prioritizes Events Captured in the Last Three Days

In the current release, the scope of the initial data warehousing job has changed. In previous releases, when this job ran on large CMS databases, CA DataMinder prioritized events captured in the last two months. Now the initial data warehousing job only prioritizes events captured in the last 3 days.

Background

CA DataMinder populates the data warehouse with event data as soon as possible after the BusinessObjects Integration feature or the iConsole dashboard have been installed or upgraded. Scheduled jobs to populate the data warehouse run automatically. In the current release, on CMSs with over 100,000 events, CA DataMinder processes events captured in the last 3 days as soon as possible after installation or upgrade. CA DataMinder then processes events older than 3 days by running daily off-peak data warehousing jobs.

In previous releases, CA DataMinder processed events captured in the last 2 months as soon as possible after installation or upgrade.

However, in all cases you can change the data warehousing job parameters and the job frequency.

Who Does This Change Affect?

This change only affects existing CA DataMinder customers who need to truncate and partition the data warehouse and who have a CMS with over 100,000 events. These customers may notice that the data warehouse takes longer to become fully populated after truncating and partitioning the data warehouse.

Note: You typically need to truncate and partition the data warehouse if you regularly purge events from you CMS database, it is likely that your data warehouse contains any events that no longer exist on the CMS. Specifically, the event participant details for these events no longer exists. Therefore these participant details cannot be processed into the Event Participant Fact table in the data warehouse. In this situation, we recommend that you truncate and repopulate the entire data warehouse to avoid discrepancies in report results.

Features No Longer Supported

The current version of CA DataMinder no longer supports the following integrations:

Symantec Enterprise Vault 7.x and 8.x

CA DataMinder no longer supports Symantec Enterprise Vault 7.x and 8.x because Symantec's standard support for theses versions has expired.

Note: CA DataMinder supports Enterprise Vault 9.0 SP1 or higher for Exchange and Domino emails.

Announcements for 14.0

This section lists important changes in version 14.0 of CA DataMinder.

Announcements:

Text Extraction By Autonomy KeyView

CA DataMinder now uses Autonomy KeyView technology to extract the text content of captured events. (Previous versions of CA DataMinder used Oracle Outside In technology.)

With the transfer to KeyView technology, there may be some differences in the extracted data compared to previous CA DataMinder releases. However, our testing indicates that any effects on the accuracy of existing user policies are negligible. Indeed, in some cases, the transfer to KeyView technology is likely to result in fewer false positives.

Impact on Fingerprinted Documents

(Only affects customers upgrading from CA DataMinder 12.5)

Content agent triggers created in CA DataMinder 12.5 continue to work when you upgrade to CA DataMinder 14.0. In general, any existing content agent triggers continue to detect documents that were fingerprinted using 12.5 content agents.

However, existing content agent triggers may fail to detect PDFs and, especially, spreadsheets that were fingerprinted using 12.5 content agents. This problem mainly affects Text Detection content agents with sentence- or paragraph-level accuracy. The problem is caused by minor discrepancies between Outside In and KeyView text extraction technologies. Specifically, the upgraded content agent triggers now use KeyView technology to analyze documents. But these triggers are comparing the documents against a content index of document signatures that was generated using Outside In technology.

To ensure that fingerprinted spreadsheets and PDFs are reliably detected after you upgrade to CA DataMinder 14.0, we recommend that you regenerate the affected content agents. Rebuild the content indexes and then republish the content agents.

FSA Rescans Unmodified Items After Upgrade

The current CA DataMinder release includes a timestamp conversion fix for the File Scanning Agent (FSA). However, this fix may cause the FSA to rescan all previously scanned items, even if they are unmodified, when you upgrade the FSA. This issue affects all existing scanning jobs that use the 'Only rescan items if they have been modified since the last scan' job option.

What causes this problem? The scanned files database contains details of files already scanned, including each file's Last Modified timestamp. However, the method used previously to convert local timestamps to UTC timestamps was incorrect. The timestamp conversion is now fixed. Therefore when you upgrade the FSA, it recalculates all UTC timestamps in the scanned files database. When a scanning job next runs, the FSA detects that all timestamps have changed and infers that all items have been modified since the last scan. Consequently, the FSA rescans all items, including files that have not been modified or updated.

Improved Bulk Auditing

Bulk auditing of events in the iConsole has been improved. Previously, if a large number of events were included in a bulk audit operation, the operation sometimes timed out before all of the events were updated. Also, the iConsole presented the user with no progress information.

In the current CA DataMinder release, bulk auditing methods have been optimized to greatly reduce the risk of timeouts. A progress dialog also tracks the number of events successfully audited and the number that were skipped. It is also now possible to cancel the auditing operation at any time.

Finally, these improvements have simplified the setup for the 'one-click review' buttons. Specifically, the 'Action If Invalid' option is no longer needed and has been removed from the Tool Buttons tab of the Audit Options dialog in the Administration console.

iConsole dashboard only supported in 32-bit browsers

You can only use the iConsole dashboard in a 32-bit browser because the required Adobe Flash is not available as a plug-in for 64-bit browsers.

Features No Longer Supported

The current version of CA DataMinder no longer supports the following features, integrations, and upgrade paths:

CA DataMinder version 5.0

The current version of CA DataMinder no longer supports upgrades from version 5.0 (when the product was known as Orchestria APM). You can only upgrade from version 6.0 or later.

Internet Explorer 6

CA DataMinder no longer supports Microsoft Internet Explorer 6 (IE6). Specifically, the CA DataMinder Internet Explorer endpoint agent no longer integrates with IE6 and the iConsole is not supported in IE6.

Note: CA DataMinder continues to support IE7, IE8, and IE9.

Autonomy Message Manager

CA DataMinder no longer supports Message Manager. Specifically, the External Agent API no longer integrates with the following versions of Message Manager:

- r12.0.1.1 Service Pack
- r12.5.1 Service Pack
- r12.6

Note: In the 14.0 server installation wizard, the Remote Data Manager Configuration screen still lists 'Autonomy Message Manager' as a supported archive. This is a known issue. There may also still be residual, redundant references to Message Manager elsewhere in the CA DataMinder 14.0 bookshelf.

Autonomy ZANTAZ Digital Safe

CA DataMinder no longer supports Digital Safe. Specifically, the Universal Adapter no longer integrates with Autonomy ZANTAZ Digital Safe 6.7.3.

IBM DB2 CommonStore

CA DataMinder no longer supports CommonStore. Specifically, the Universal Adapter no longer integrates with IBM DB2 CommonStore 8.3 for Exchange or Domino.

Symantec Enterprise Vault 6.0 SP3

CA DataMinder no longer supports Enterprise Vault 6.0 SP3. Specifically, the EV archive agent, wgnsev.dll, no longer integrates with Enterprise Vault 6.0 SP3.

Note: If using Enterprise Vault to archive:

- Exchange emails, CA DataMinder supports Enterprise Vault 7.0 or higher.
- Domino emails, CA DataMinder supports Enterprise Vault 9.0 SP1.

EMC SourceOne Email Management 6.5 SP1

CA DataMinder no longer supports EMC SourceOne 6.5 SP1. Specifically, the SourceOne archive agent, wgnemcs1.dll, no longer integrates with EMC SourceOne 6.5 SP1.

Note: CA DataMinder supports SourceOne 6.6 SP1.

Personal Audit Report (PAR)

The Personal Audit Report is no longer included in the standard reports available for CA DataMinder.

Instead, reviewers can edit the properties of the Compliance Audit Report to retrieve details about their own workload statistics (how many events are assigned to them for review, how many they have already reviewed, and so on).

Secure Private Tunnel (SPT)

CA DataMinder no longer supports the Secure Private Tunnel.

IM Dump File Formats

The following dump file formats are no longer supported by the IM import utility, IMFrontEnd.exe:

- MindAlign: A proprietary XML data format for Parlano MindAlign IM servers.
- MindAlign-IC3: A customized variation on the MindAlign format—see above.
- Unified ibbloomberg: A 'short format' dump file for Bloomberg messages.
- Unified ibinet: A 'long format' dump file for Bloomberg messages.
- Unified instantbb: A dump file format for Bloomberg instant messaging data.
- DirBBEmailXML: An XML format dump file for archived Bloomberg messages.

Note: CA DataMinder continues to support:

However, IMFrontEnd.exe continues to support the following formats:

- FaceTime: A proprietary XML format for Actiance IM data. The corresponding data source parameter is DirFaceTime.
- DirIBXML: A proprietary XML format for Instant Bloomberg messages.
- IMlogic: A proprietary XML format for IMlogic instant messaging data. The corresponding data source parameter is DirIMLogic.

Note: You must first configure IM Manager to convert IMlogic dump files into a format supported by IMFrontEnd.exe.

FastStart Policies

The following web-targeted policies are no longer included in the CA DataMinder Standard Policy Pack:

- Blogging/Messaging Sites
- Wiki Posting Control
- Social Networking

Transaction Detector Triggers

Triggers to detect monetary transactions (such as online purchases) are no longer supported.

These triggers were previously available in Web Page and email versions.

Transaction Events

In previous versions of CA DataMinder, it was possible to capture or control transaction-specific events. This capability is no longer supported.

MSIZAP.EXE

The Microsoft Windows Installer Cleanup utility is no longer provided on the distribution media.

Chapter 6: New Features

This section contains the following topics:

Features Added in 14.6

This section describes the new features added in CA DataMinder 14.6.

New Features:

Integration with IBM Content Collector

CA DataMinder can integrate with IBM Content Collector V3.0 and V4.0. This integration enables you to apply smart tags to emails stored in Content Collector. You can also use the CA DataMinder iConsole or Data Management console to search for these archived emails.

Note: Integration between CA DataMinder and Content Collector is based on a CA DataMinder archive agent. For full details, see the IBM Content Collector Integration chapter in the *Archive Integration Guide*.

Support for Microsoft Exchange Server 2013

The Exchange Server Agent can analyze and apply policy to emails passing through Microsoft Exchange Server 2013.

Note: For full details, see the Exchange, Domino, and IIS SMTP Integration chapter in the *Message Server Integration Guide*.

New Features

Outlook endpoint agent

The Outlook endpoint agent no longer captures duplicates of email attachments.

The Outlook endpoint agent can now capture RMS-restricted emails.

Event Import

Event Import can import emails from journal mailboxes on Exchange 2013 servers.

iConsole

You can prevent the iConsole from showing events of the health-monitor mailbox. Follow the instructions from Microsoft's kb article 2823959.

Exchange Server Agent

The Exchange Server Agent can now integrate with Exchange Server 2013 CU3.

Enhancements to support Exchange Server 2013

WgnCred

You can use the WgnCred.exe command utility to set Proxy Server credentials.

WgnCheck

WgnCheck.exe diagnostic command utility collects Microsoft Exchange Data and Transport DLLs to help resolve any integration errors with the environment.

More information:

Microsoft Exchange Server 2013 CU3 Certification (see page 17)

iConsole Duplicate Event Rollup

You can now customize a Standard Search to list duplicate events with certain criteria, and then do bulk auditing on the results.

Note: For more information, see the Searching for Events chapter of the *CA DataMinder iConsole User Guide*.

Regionalized Policy Engine Lookup

If you have policy engines in different regions using different user groups, you can now use the %region% attribute to distinguish PEs by location, and define conditional commands for each region.

Note: For more information about User Attribute Lookup, see the Data Lookup chapter in the *Policy Guide*.

Apply Email Policies to Sent-On-Behalf User

When user A grants "Send On Behalf" email permissions to delegate B, CA DataMinder now applies policy to user A by default. In previous releases, policy was applied to delegate B. You can now also use the %sentonbehalf% user attribute in lookup commands explicitly.

Note: For more information about User Attribute Lookup, see the Data Lookup chapter in the *Policy Guide*.

Features Added in 14.5

This section describes the new features added in CA DataMinder 14.5.

New Features:

Integration with File Sync Providers

In the current release, CA DataMinder has extended its Data In Use protection capabilities and can now prevent unauthorized file syncing. By default, CA DataMinder can apply policy to files being synced to:

- Box
- DropBox
- Google Drive
- Microsoft SkyDrive

Supported File Sync Methods

File sync providers typically provide two sync methods:

- Users can install a Windows Explorer plug-in on their workstation. This plug-in is the 'file sync application'. The user launches Windows Explorer and drags the file that they want to share into the sync folder.
- Users can log in to file sync web site (such as DropBox.com) and upload the file that they want to share into the sync folder.

CA DataMinder provides Data In Motion protection for both file sync methods.

How Does CA DataMinder Protect Files in Sync Folders?

If the user drags a file into their sync folder in Windows Explorer, the CFSA applies machine policy in real time. Machine policy settings determine whether the file sync application is under policy control. If it is, the CFSA applies Data In Motion triggers to analyze the file being synced.

If the user uploads a file to a file sync website, the CFSA applies Data In Motion triggers immediately.

In both cases, you can configure Data In Motion triggers to block the file sync operation. Alternatively, if the user is using a file sync application, you can set up triggers to warn the user. Or you can allow the file sync operation but categorize or encrypt the file (the user must supply a decryption password).

Note: For full details about CFSA integration with file sync applications, see the *Endpoint Integration Guide*.

NBA Supports IPv6 Networks

CA DataMinder Network can now decode traffic within IPv6 networks. IPv6 is the latest revision of the Internet Protocol (IP) that uses 128-bit addresses.

- CA DataMinder Network (Bivio Platform and Linux Server Platform) was extended to support filtering, decoding, and controlling of IPv6 in its various forms.
- The web interface has been updated to support IPv6.
- The interface to the policy engines (except on Bivio 7000) has been updated to support IPv6.

Decryption of Voltage Emails

In the current release, CA DataMinder can detect, analyze, and apply policy to emails encrypted by Voltage SecureMail.

How does the integration work? CA DataMinder intercepts Voltage-encrypted emails passing through an email server and passes copies of these emails to a CA DataMinder policy engine. The policy engine establishes a secure connection to the Voltage SecureMail server, which provides the policy engine with an unencrypted version of the email. The policy engine can then apply policy triggers to the email as normal. When policy processing is complete, the policy engine calls back to the email server agent. The callback instructs the email server agent to either block the encrypted email or allow it to continue.

For details about setting up policy engines to integrate with Voltage SecureMail, see the *Platform Deployment Guide*.

Client Network Agent

The current CA DataMinder release includes the Client Network Agent. You can use the Client Network Agent (or 'network agent') to control web activity on endpoint computers. Specifically, the network agent can monitor HTTP requests. This activity includes attempts to post files and comments to web sites or to submit form data. It can also monitor attempts to check in files to SharePoint libraries.

To configure the network agent, you edit Data In Motion triggers in the user policy. The network agent supports the Block intervention option. If required, you can configure the network agent to ignore network activity in specific applications or browsers. You specify the applications and browsers in the machine policy.

By default, the network agent is configured to monitor web activity for most common browsers and Microsoft Office applications, including Microsoft Internet Explorer, Mozilla Firefox, Opera, and Google Chrome.

How does the network agent differ from the Internet Explorer agent?

In previous versions of CA DataMinder, the Internet Explorer agent could only apply policy to web activity in Internet Explorer browsers. It applied Web triggers and could apply the full range of control actions, including Warn actions.

The network agent can apply policy to network activity in any browser and applies Data In Motion triggers. It does not support Warn control actions. Also, Data In Motion triggers offer greater file detection capabilities and also support Data Lookup commands.

Note: Unlike the Internet Explorer agent, the network agent cannot apply policy to file downloads.

How does the network agent differ from the CA DataMinder Network?

The CA DataMinder Network (NBA) operates at the network boundary and monitors outbound and inbound traffic. It runs on a dedicated Bivio hardware device or a dedicated Linux server. The NBA can also monitor traffic sent using multiple protocols, including SMTP and FTP. In particular, the NBA is able to differentiate webmails and apply Outgoing Email triggers.

The client network agent runs on users' workstations and monitors outbound network activity. Also, in the current release it can only monitor HTTP traffic.

For full details, see the Client Network Agent chapter in the *Endpoint Integration Guide*.

Simplified Configuration for the Data Warehouse

You can now configure the Data Warehouse in the Administration console. For example, you can:

- Enable or disable the Data Warehouse.
- Enable or disable the collection of event participant data. (You must collect event participant data if you intend to run BusinessObjects reports.)
- Configure the initial processing job that populates the data warehouse with event and audit data.
- Configure off-peak processing jobs.

You can also use the Administration console to add or modify credentials for the Reporting User database account.

For full details, see the Administration console online help or the Data Warehouse chapter of the *Platform Deployment Guide*.

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

New Administration Features for iConsole

The iConsole now supports extra administration features:

User Administration

You can now 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.

You can also 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.

BusinessObjects Enterprise Integration Setup

The BOE Integration component enables the iConsole to log on to BusinessObjects Enterprise and retrieve available BusinessObjects reports for CA DataMinder. You can now configure this component directly from the iConsole.

For full details, see the iConsole online help or the Administration chapter of the *iConsole User Guide*.

FSA Database Scanning Enhancements

FSA database scanning has been improved to be row and column aware. The analysis has been improved to find information sets (for example, firstname + last name + SSN) across the same row, instead of across all rows, which lowers the number of false positives.

You as the DBA can now trace back violations by their primary key in the iConsole, and the iConsole highlights rows that matched, so you can find them more easily.

Other New Features

The following new features have also been added to CA DataMinder since 14.1.

New Security Model: 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.

Client File Server Agent can protect files on SD cards

The CFSA can now apply policy to files being copied to SD cards.

Protection for SD cards works in exactly the same way as CFSA protection for USB removable devices. In both cases, the CFSA applies Data In Motion triggers to files being copied. The available control actions (for example, blocking or encryption) are also the same.

Windows Server 2012

CMSs and gateway servers now support Microsoft Windows Server 2012.

A full list of supported operating systems is in the Requirements chapter of the *Platform Deployment Guide*.

Windows 8

Endpoint agents now support Microsoft Windows 8.

A full list of supported operating systems is in the Requirements chapter in the *Endpoint Integration Guide*.

Exchange Server 2013

CA DataMinder can now analyze and apply policy to emails passing through Microsoft Exchange Server 2013.

But see also the support limitations (see page 19).

Outlook 2013

CA DataMinder can now analyze and apply policy to incoming and outgoing emails in Microsoft Outlook 2013.

Office 2013

CA DataMinder can now analyze and apply policy to files created using Microsoft Office 2013 applications.

SharePoint 2013

The CA DataMinder File Scanning Agent can now scan files and documents stored on SharePoint 2013 sites.

CA Business Intelligence 3.3

CA DataMinder now integrates with BusinessObjects XI 3.1 SP5. In fact, CA DataMinder integration with BusinessObjects Enterprise now *requires* BusinessObjects XI 3.1 SP5! Specifically, SP4 is no longer supported.

Compatibility with CA products is provided through CA Business Intelligence. CA Business Intelligence is a wrapper that includes a BusinessObjects Enterprise installation. The current CA DataMinder release supports CA Business Intelligence 3.3. When you install CA Business Intelligence 3.3 on your reports server, BusinessObjects XI 3.1 SP5 and its InfoView web portal also get installed.

User Policies Export

You can now export user policies to a human-readable spreadsheet by running a wgninfra.exe command, or from the File, Export Policy Blueprint menu in the User Policy Editor.

Support for regional archives

CA DataMinder supports multiple unconnected email archive instances on a single Central Management Server. If your enterprise has separate installations of the same email archive in multiple geographic regions, it is now possible to segregate the events from these onto a single CMS so that the Remote Data Manager can retrieve historic emails from the correct archive installation. See CA DataMinder Archive Integration Guide, Third-Party Integration for more details.

Features Added in 14.1

This section describes the new features added in CA DataMinder 14.1.

New Features:

Binary Text Extractor (see page 46)
Exempt Users (see page 46)
Role-Based iConsole Configuration (see page 47)
Other New Features (see page 47)

Binary Text Extractor

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

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

Configuration details for the Binary Text Extractor are saved in BinaryTextorConfig.xml. You edit this file manually to specify the file types that you want CA DataMinder to analyze. Configuration instructions and details about the supported XML schema are in the *Platform Deployment Guide*.

Exempt Users

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.

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

You can exempt user accounts manually in the Administration console. You can also exempt users automatically 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.

Configuration instructions for exempt users are in the *Administration Guide*. Account Import instructions are in the *Platform Deployment Guide*.

Role-Based iConsole Configuration

You can configure the iConsole separately for different user roles. For each role, you can specify which settings, portlets, searches, and reports are available to users when they use the iConsole.

For example, an administrator has added two new user roles, HR Reviewers and PII Reviewers. In the iConsole, the administrator can assign separate searches to each role. The searches available to HR Reviewers focus on emails captured by Employee Behavior policies in the standard policy pack. Conversely, searches available to PII Reviewers focus on emails captured by Personally Identifiable Information policies.

Likewise, you can configure iConsole settings and portlets to allow Administrators to define their own personal home pages but prevent other users from doing so.

Instructions for setting up role-based iConsole configurations are in the *iConsole User Guide* and iConsole online help.

Other New Features

The following new features have also been added to CA DataMinder since 14.0.

Up to 10 Audit Buttons

The current CA DataMinder release supports up to ten configurable, audit buttons  in the iConsole.

Previously, administrators could only configure five audit buttons.

Symantec Enterprise Vault 10

CA DataMinder can integrate with the Enterprise Vault 10 when it is being used to archive emails.

This version is in addition to existing CA DataMinder support for Enterprise Vault 9.0 SP1.

The CA DataMinder installer detects which version of Enterprise Vault you are using and installs an appropriate version of the EV archive agent. However, if you later upgrade to Enterprise Vault 10 from an earlier version, you must also upgrade your CA DataMinder integration to use the correct version of the EV archive agent.

Details are in the *Archive Integration Guide*. See the 'Integration Requirements' section in the Symantec Enterprise Vault Integration chapter.

EMC SourceOne 6.7 and 6.8

CA DataMinder can now integrate with EMC Source One 6.7 and 6.8.

These versions are in addition to existing CA DataMinder support for EMC SourceOne 6.6 SP1.

SQL Server 2012

The CMS and gateways now support SQL Server 2012 databases.

For the full list of supported databases, see the *Database Guide*.

FSA Database Scans for SQL Server 2012

The File Scanning Agent can now scan records in SQL Server 2012 databases.

The full list of supported databases includes:

- Microsoft SQL Server 2005, 2008, and 2012
- Oracle 10g (10.2.0.4), and 11g (11.1.0.7) or later

'CustomRoleUpgrade' Utility

CA DataMinder provides a post-upgrade 'CustomRoleUpgrade' utility to create new user roles that correspond to any custom combinations of administrative privileges held by your users. You can use this utility to assign users without a recognized role to an equivalent 'official' user role. In turn, this allows you to customize the iConsole for these users by implementing the new role-based iConsole configuration (see page 47).

For details, see the 'Automatically Reassign Users with Custom Roles to Equivalent 'Official' Roles' section in the *Upgrade Guide*.

Features Added in 14.0

This section describes the new features added in version 14.0 of CA DataMinder.

New Features:

CA DataMinder Network Enhancements

CA DataMinder has released a 14.0 version of the Network agent on Linux servers.

Previously, CA DataMinder only supported a r12.5 version of the Network agent on Bivio 2000 and Bivio 7000 appliances. (However, this version of the network agent was supported for use with other CA DataMinder 14.0 components.)

For details about CA DataMinder Network 14.0, see CA DataMinder Network Release Notes.

BusinessObjects Enterprise Reports for CA DataMinder

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

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.

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.

You can access BusinessObjects reports for CA DataMinder directly from the iConsole Review tab. You can also launch InfoView from a link in the iConsole. You can then create, schedule and run CA DataMinder reports from the InforView itself. Alternatively, you can browse directly to InfoView.

Note: CA DataMinder integration with BusinessObjects Enterprise is described in the *Reports Integration Guide*.

Content Searches

CA DataMinder has reintroduced the 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.

To enable content searches, you must first index CA DataMinder events into a content database using the content indexer. This utility extracts CA DataMinder events from the CMS and submits them to the content database. The content database then processes these events, storing them as indexed, text-searchable documents. When a reviewer runs a content search, the content database analyzes the indexed documents and returns all documents that match the search criteria.

Notes

- If you used content searches in an earlier version of CA DataMinder, be aware that the More Like This option is no longer available in the Content Search Results screen.
- The current CA DataMinder release uses content database technology provided by Autonomy IDOL. You can install the IDOL content database included with CA DataMinder or you can use an existing IDOL content database.

IDOL Content Indexing Not Intended To Support High Capture Rate

Content indexing in the current version of CA DataMinder uses Autonomy IDOL technology.

Content indexing based on Autonomy IDOL technology enhances the violation review capabilities for customers who need to:

- Capture a sub-set of an organization's overall information content
- Retain this information content for relatively short periods (for example, one year).

Content indexing using Autonomy IDOL technology is not intended to support high capture rates that would result in substantial volumes of data in the CMS database with long retention periods. CA DataMinder deployments that require Autonomy IDOL installations of significant scale are best served by leveraging the CA DataMinder Content Connector API. Using this API, third party content indexing solutions (including a separately licensed Autonomy IDOL) can consume CA DataMinder data directly and can be scaled independently to meet such requirements.

iConsole Screens Redesigned

The iConsole screens have been redesigned to be easier to use, consistent with other CA products, and to comply with Section 508 Accessibility requirements.

In particular, the iConsole now uses a tabbed layout, allowing fast access to Review, Policy and Administration tasks and features.

Users can now create a home page and add portlets to it. Portlets can be customized and users can set them up to display the information that they access most commonly.

Settings for individual searches and reports are organized into Properties tabs. Toolbars have also been redesigned and a new toolbar has been added to search results screens.

Other New Features

The following new features have also been added to CA DataMinder since r12.5.

Support for Internet Explorer 9

The current CA DataMinder release supports Microsoft Internet Explorer 9 (IE9)

- The Internet Explorer endpoint agent now integrates with IE9.
- The iConsole now runs in IE9.

Support for Symantec Enterprise Vault for Domino

CA DataMinder can integrate with the Symantec Enterprise Vault archive solution when it is being used to archive Domino emails.

Specifically, the EV archive agent can now process emails extracted from Lotus Domino journals.

Bookshelf Reorganization

The CA DataMinder bookshelf has been reorganized. In particular, the former *Deployment Guide* has been replaced by the following guides:

- *Platform Deployment Guide*. This guide covers key deployment tasks including: CMS and gateway deployment; Account Import; policy engine deployment; iConsole deployment; content registration agents; content indexing; and the Quarantine Manager. This guide also includes any other sections previously in the *Deployment Guide* and which are not covered by the new integration guides.
- *Archive Integration Guide*. This guide includes: Event Import; IM Import; CA DataMinder integration with third party archive solutions; Remote Data Manager; the Universal Extractor; and the ICAP agent.
- *Endpoint Integration Guide*. This guide covers the CA DataMinder endpoint agents, including: the Outlook, Notes, and Internet Explorer agents; the Client File System Agent (CFSA); and the Client Print System Agent (CPSA).
- *Message Server Integration Guide*. This guide covers the Exchange and Domino email server agents, plus the Milter MTA and IIS SMTP agents.
- *Stored Data Server Integration Guide*. This guide covers the File Scanning Agent (FSA).

The current bookshelf also includes the *Administration Guide* and *iConsole User Guide*. These guides were omitted from recent versions of CA DataMinder but have now been restored.

Reports Integration Guide

This guide is a new addition to the CA DataMinder bookshelf and describes the CA DataMinder integration with BusinessObjects Enterprise. The guide covers deployment and how to manage BusinessObjects reports for CA DataMinder in the iConsole and the InfoView web portal.

Chapter 7: Hotfixes Included In This Release

This section contains the following topics:

Hotfixes Included in 14.6

CA DataMinder 14.6 incorporates the following hotfixes issued since 14.5. The list includes the APAR number for each hotfix.

- Client_14.5_HF017.msp (RO67094)
- Client_x64_14.5_HF018.msp (RO67094)
- Integration_x64_14.5_HF005.msp (RO66229)
- Integration_x64_14.5_HF016.msp (RO66288)
- Integration_x64_14.5_HF013.msp (RO66287)
- Reports_patch_14_5_70438.msp (RO66386)
- Reports_14.5_HF010.msp (RO66386)
- Server_14.5_HF011.msp (RO66233)
- Server_x64_14.5_HF004.msp (RO60702)
- Server_x64_14.5_HF007.msp (RO66420)
- Server_x64_14.5_HF009.msp (RO66290)
- Server_14.5_HF013.msp (RO67570)
- Server_x64_14.5_HF014.msp (RO67570)
- Server_14.5_HF014.msp (RO66286)
- Server_x64_14.5_HF015.msp (RO66286)
- Sevddup_14.5_HF006.msp (RO65796)
- Web_14.5_HF003.msp (RO60503)

For details about these hotfixes, see the readme files that accompanied the hotfixes. The hotfixes and readme files are available from CA Technical Support: http://ca.com/support

Note: All releases are cumulative. Fixes included in this release incorporate and supersede fixes in earlier releases.

Hotfixes Included in 14.5

CA DataMinder 14.5 incorporates the following hotfixes issued since 14.1. The list includes the APAR number for each hotfix.

For details about these hotfixes, see the readme files that accompanied the hotfixes. The hotfixes and readme files are available from CA Technical Support: http://ca.com/support

Note: All releases are cumulative. Fixes included in this release incorporate and supersede fixes in earlier releases.

Hotfix originally issued for CA DLP 12.0

- Server_12.0_HF081 (RO46137)

Hotfixes originally issued for CA DLP 12.5

- NBA_12.5_2629.0 (RO50718)
- Server_12.5_HF0136 (RO46415)
- Integration_12.5_HF0137 (RO46415)
- Integration_x64_12.5_HF0138 (RO46415)
- Server_12.5_HF0146 (RO46981)
- Web_12.5_HF0147 (RO47383)
- Web_12.5_HF0148 (RO47482)
- Server_12.5_HF0149 (RO47960)
- Integration_12.5_HF0150 (RO48756)
- Integration_x64_12.5_HF0151 (RO48756)
- Client_x64_12.5_HF0153 (RO48588)
- Server_12.5_HF0154 (RO49139)
- Reports_12.5_HF0157 (RO49855)
- Web_12.5_HF0158 (RO51049)
- Server_12.5_HF0159 (RS51710)
- Client_12.5_HF0160 (RS51710)
- Client_x64_12.5_HF0161 (RS51710)
- Web_12.5_HF0164 (RO52498)

- Reports_12.5_HF0165 (RO52499)
- Client_12.5_HF0166 (RO52767)
- Integration_12.5_HF0168 (RO55396)
- Integration_x64_12.5_HF0169 (RO55396)
- Server_12.5_HF0170 (RO54466)
- Web_12.5_HF0171 (RO54481)
- Integration_12.5_HF0172 (RO55146)
- Integration_x64_12.5_HF0173 (RO55146)
- Server_12.5_HF0174 (RO55146)

Hotfixes originally issued for CA DLP 14.0

- NBA_14.0_2807.0 (RO50721)
- Web_14.0_HF031 (RO46961)
- Server_14.0_HF032 (RO46476)
- Web_14.0_HF033 (RO47387)
- Client_14.0_HF034 (RO47947)
- Client_x64_14.0_HF035 (RO47947)
- Integration_14.0_HF037 (RO47895)
- Integration_x64_14.0_HF038 (RO47895)
- BOXI_14.0_HF040 (RO49811)
- Server_14.0_HF041 (RO48946)
- Server_14.0_HF042 (RO49710)
- Integration_x64_14.0_HF043 (RO49332)
- Server_14.0_HF044 (RO50145)
- Server_14.0_HF045 (RO50486)
- Server_14.0_HF046 (RO51399)
- Server_14.0_HF047 (RO51757)
- Reports_14.0_HF048 (RO51760)
- Server_14.0_HF049 (RO51711)
- Web_14.0_HF050 (RO51647)
- Reports_14.0_HF051 (RO52001)

- Integration_14.0_HF052 (RO51998)
- Integration_x64_14.0_HF053 (RO51998)
- Reports_14.0_HF054 (RO52212)
- Web_14.0_HF055 (RO52211)
- Server_14.0_HF056 (RO54063)
- Server_14.0_HF059 (RO54248)
- Server_14.0_HF060 (RO54253)
- Integration_14.0_HF061 (RO55147)
- Integration_x64_14.0_HF062 (RO55147)
- Server_14.0_HF063 (RO55147)

Hotfixes originally issued for CA DataMinder 14.1

- Client_14.1_HF004 (RO54021)
- Client_x64_14.1_HF005 (RO54021)
- Integration_14.1_HF006 (RO54339)
- Integration_x64_14.1_HF007 (RO54339)

Hotfixes Included in 14.1

CA DataMinder 14.1 incorporates the following hotfixes issued since 14.0. The list includes the APAR number for each hotfix.

For details about these hotfixes, see the readme files that accompanied the hotfixes. The hotfixes and readme files are available from CA Technical Support: http://ca.com/support

Note: All releases are cumulative. Fixes included in this release incorporate and supersede fixes in earlier releases.

- Client_14.0_HF003 (RO40803)
- Client_x64_14.0_HF004 (RO49811)
- Web_14.0_HF005 (RO48601)
- Server_14.0_HF006 (RO38336)
- BOXI_14.0_HF007 (RO41912)

- Web_14.0_HF012 (RO45070)
- Server_14.0_HF013 (RO47947)
- Client_14.0_HF014 (RO38336)
- Client_x64_14.0_HF015 (RO41912)
- Web_14.0_HF016 (RO45070)
- Server_14.0_HF018 (RO47947)
- Server_14.0_HF018 (RO47895)
- Web_14.0_HF023 (RO51998)
- Server_14.0_HF024 (RO47895)
- Client_14.0_HF025 (RO49332)
- Client_x64_14.0_HF026 (RO51998)
- Server_14.0_HF027 (RO51760)
- Web_14.0_HF029 (RO52001)
- Server_14.0_HF030 (RO52212)
- Web_14.0_HF031 (RO40803)
- Server_14.0_HF032 (RO41912)
- Web_14.0_HF033 (RO43471)
- Client_14.0_HF034 (RO43471)
- Client_x64_14.0_HF035 (RO45070)
- CCS_x64_14.0_HF036 (RO45444)
- Integration_14.0_HF037 (RO45119)
- Integration_x64_14.0_HF038 (RO46476)
- BOXI_14.0_HF040 (RO48946)
- Server_14.0_HF041 (RO50145)
- Integration_x64_14.0_HF043 (RO50486)
- Server_14.0_HF044 (RO51399)
- Server_14.0_HF045 (RO51757)
- Server_14.0_HF046 (RO51711)
- Server_14.0_HF047 (RO38373)
- Reports_14.0_HF048 (RO41355)

- Server_14.0_HF049 (RO42127)
- Web_14.0_HF050 (RO44518)
- Reports_14.0_HF051 (RO45116)
- Integration_14.0_HF052 (RO46961)
- Integration_x64_14.0_HF053 (RO47387)
- Reports_14.0_HF054 (RO51647)
- Web_14.0_HF055 (RO52211)

Hotfixes Included in 14.0

CA DataMinder 14.0 incorporates the following hotfixes issued since r12.5. The list includes the APAR number for each hotfix.

For details about these hotfixes, see the readme files that accompanied the hotfixes. The hotfixes and readme files are available from CA Technical Support: http://ca.com/support

Note: All releases are cumulative. Fixes included in this release incorporate and supersede fixes in earlier releases.

- Web_12.5_HF001 (RO25182)
- Web_12.5_HF002 (RO25418)
- Integration_12.5_HF006 (RO25556)
- Integration_x64_12.5_HF007 (RO25556)
- Server_12.5_HF008 (RO25557)
- Client_12.5_HF009 (RO25557)
- Integration_12.5_HF004 (RO25420)
- Integration_x64_12.5_HF005 (RO25420)
- Server_12.5_HF003 (RO25420)
- Client_x64_12.5_HF010 (RO25557)
- Client_12.5_HF011 (RO25517)
- Client_x64_12.5_HF012 (RO25517)
- Client_12.5_HF014 (RS25484)
- Client_x64_12.5_HF015 (RS25484)
- Server_12.5_HF013 (RS25484)

- Integration_12.5_HF016 (RS25484)
- Integration_x64_12.5_HF017 (RS25484)
- Client_12.5_HF018 (RO25517)
- Client_x64_12.5_HF019 (RO25517)
- Client_12.5_HF024 (RO26125)
- Support_12.5_HF020 (RO26969)
- Integration_12.5_HF021 (RO25844)
- Integration_x64_12.5_HF022 (RO25844)
- Web_12.5_HF023 (RO25855)
- Client_x64_12.5_HF025 (RO26125)
- Server_12.5_HF026 (RO26840)
- Web_12.5_HF027 (RO27449)
- Client_12.5_HF028 (RO27746)
- Client_x64_12.5_HF029 (RO27746)
- Server_12.5_HF030 (RO28695)
- Server_12.5_HF031 (RO29212)
- Reports_12.5_HF032 (RO28464)
- Integration_12.5_HF047 (RO31813)
- Server_12.5_HF033 (RO29075)
- Web_12.5_HF034 (RO29076)
- Server_12.5_HF035 (RO29974)
- Web_12.5_HF036 (RO29975)
- Server_12.5_HF037 (RO30865)
- Client_12.5_HF038 (RO31159)
- Client_x64_12.5_HF039 (RO31159)
- Web_12.5_HF040 (RO31002)
- Web_12.5_HF044 (RO32174)
- Reports_12.5_HF045 (RO32174)
- Web_12.5_HF046 (RO31718)
- Integration_12.5_HF047 (RO31813)

- Integration_x64_12.5_HF048 (RO31813)
- Server_12.5_HF049 (RO31760)
- Web_12.5_HF050 (RO32863)
- Server_12.5_HF053 (RO32321)
- Server_12.5_HF054 (RO32461)
- Integration_12.5_HF055 (RO32461)
- Integration_x64_12.5_HF056 (RO32461)
- Integration_12.5_HF057 (RO33144)
- Integration_x64_12.5_HF058 (RO33144)
- Client_12.5_HF059 (RO33071)
- Client_x64_12.5_HF060 (RO33071)
- Reports_12.5_HF064 (RO33492)
- Web_12.5_HF065 (RO33745)
- Web_12.5_HF066 (RO33891)
- Client_12.5_HF067 (RO34097)
- Client_x64_12.5_HF068 (RO34097)
- Server_12.5_HF069 (RO34211)
- Web_12.5_HF070 (RO34560)
- Server_12.5_HF071 (RO34547)
- Web_12.5_HF072 (RO34684)
- Web_12.5_HF073 (RO34560)
- Server_12.5_HF074 (RO35193)
- Client_12.5_HF075 (RO35193)
- Client_x64_12.5_HF076 (RO35193)
- Server_12.5_HF077 (RO34591)
- Integration_12.5_HF078 (RO34591)
- Integration_x64_12.5_HF079 (RO34591)
- Server_12.5_HF080 (RO34576)
- Web_12.5_HF082 (RO36123)
- Server_12.5_HF083 (RO35717)

- Server_12.5_HF084 (RO36448)
- Client_12.5_HF085 (RO36448)
- Client_x64_12.5_HF086 (RO36448)
- Client_12.5_HF087 (RO36562)
- Client_x64_12.5_HF088 (RO36562)
- Integration_12.5_HF092 (RO36933)
- Integration_x64_12.5_HF093 (RO36933)
- Server_12.5_HF094 (RO36564)
- Integration_12.5_HF099 (RO37270)
- Integration_x64_12.5_HF0100 (RO37270)
- Server_12.5_HF0101 (RO36879)
- Client_12.5_HF0102 (RO36879)
- Client_x64_12.5_HF0103 (RO36879)
- Server_12.5_HF0110 (RO38189)
- Server_12.5_HF0111 (RO37884)
- Client_12.5_HF0112 (RO37884)
- Client_x64_12.5_HF0113 (RO37884)
- Web_12.5_HF0125 (RO42472)

Hotfixes Included in 12.5

CA DataMinder 12.5 incorporates the following hotfixes issued since 12.0. The list includes the APAR number for each hotfix.

For details about these hotfixes, see the readme files that accompanied the hotfixes. The hotfixes and readme files are available from CA Technical Support: http://ca.com/support

Note: All releases are cumulative. Fixes included in this release incorporate and supersede fixes in earlier releases.

- Client_12.0_Advanced Encryption (RO16355)
- Web_12.0_HF001 (RO12553)
- Server_12.0_HF004 (RO13268)
- Web_12.0_HF007 (RO14187)
- Server_12.0_HF012 (RO15122)

- Server_12.0_HF016 (RO15388)
- Integration_12.0_HF017 (RO15388)
- Web_12.0_HF018 (RO15392)
- Server_12.0_HF019 (RO15634)
- Server_12.0_HF020 (RO15453)
- Web_12.0_HF023 (RO15637)
- Web_12.0_HF024 (RO16544)
- Server_12.0_HF025 (RO16080)
- Server_12.0_HF026 (RO16543)
- Server_12.0_HF028 (RO20091)
- Integration_x64_12.0_HF029 (RO20090)
- Ua_12.0_HF030 (RO20092)
- Reports_12.0_HF031 (RO18119)
- Reports_12.0_HF032 (RO18119)
- Reports_12.0_HF033 (RO18680)
- Server_12.0_HF034 (RO19138)
- Server_12.0_HF035 (RO19518)
- Integration_12.0_HF036 (RO19458)
- Client_12.0_HF037 (RO19499)
- Server_12.0_HF041 (RO20444)
- Server_12.0_HF043 (RO20767)
- Reports_12.0_HF044 (RO20767)
- Server_12.0_HF045 (RO21147)
- Server_12.0_HF045 (RO21147)
- Web_12.0_HF046 (RO21147)
- Server_12.0_HF049 (RO21447)
- Reports_12.0_HF050 (RO21448)
- Server_12.0_HF051 (RO21907)
- Client_12.0_HF052 (RO21908)
- Server_12.0_HF053 (RO23424)

- Server_12.0_HF054 (RO23907)
- Client_12.0_HF055 (RO23908)
- Reports_12.0_HF056 (RO23425)
- Web_12.0_HF057 (RO24870)
- Server_12.0_HF059 (RO25419)
- Server_12.0_HF059 (RO25419)
- Integration_12.0_HF060 (RO25419)
- Reports_12.0_HF061 (RO24928)
- Client_12.0_HF062 (RO25183)
- Server_12.0_HF063 (RO25246)
- Server_12.0_HF064 (RO26195)
- Web_12.0_HF065 (RO26146)
- Reports_12.0_HF066 (RO26263)
- Server_12.0_HF067 (RO26626)
- Client_12.0_HF068 (RO26626)
- Server_12.0_HF069 (RO26839)
- Reports_12.0_HF070 (RO27448)
- Server_12.0_HF071 (RO27450)
- Integration_12.0_HF072 (RO29275)
- Client_12.0_HF073 (RO29074)
- Integration_x64_12.0_HF074 (RO29131)
- Server_12.0_HF075 (RO30657)
- Client_12.0_HF076 (RO30657)
- Integration_12.0_HF077 (RO30657)
- Server_12.0_HF078 (RO30965)
- Server_12.0_HF079 (RO30812)
- Client_12.0_HF080 (RO30812)
- Server_12.0_HF081 (RO46137)

Hotfixes Included in 12.0

CA DataMinder 14.5 incorporates the following hotfixes issued since 14.1. The list includes the APAR number for each hotfix.

For details about these hotfixes, see the readme files that accompanied the hotfixes. The hotfixes and readme files are available from CA Technical Support: http://ca.com/support

Note: All releases are cumulative. Fixes included in this release incorporate and supersede fixes in earlier releases.

- Client_6.0_HF102 (RO09874)
- Server_6.0_HF104 (RO09884)
- Client_6.0_HF105 (RO09875)
- Server_6.0_HF106 (RO09885)
- Server_6.0_HF109 (RO09886)
- Server_6.0_HF110 (RO09887)
- Integration_6.0_HF111 (RO09882)
- Server_6.0_HF112 (RO09888)
- Client_6.0_HF113 (RO09876)
- Integration_6.0_HF114 (RO09883)
- Server_6.0_HF115 (RO09889)
- Client_6.0_HF116 (RO09877)
- Client_6.0_HF117 (RO09878)
- Server_6.0_HF121 (RO09890)
- Server_6.0_HF121 (RO09890)
- Client_6.0_HF122 (RO09879)
- Client_6.0_HF125 (RO09880)
- Web_6.0_HF126 (RO09892)
- Server_6.0_HF127 (RO09891)
- Client_6.0_HF128 (RO09881)

- Server_6.0_HF129 (RO12262)
- Integration_6.0_HF130 (RO12266)
- Server_6.0_HF131 (RO12551)
- Integration_6.0_HF132 (RO12551)
- Server_6.0_HF133 (RO12552)
- Server_6.0_HF135 (RO13267)
- Server_6.0_HF136 (RO17244)
- Server_6.0_HF137 (RO18668)
- Client_6.0_HF138 (RO18670)
- Server_6.0_HF139 (RO21909)
- Server_6.0_HF140 (RS25385)
- Integration_6.0_HF141 (RS25385)
- Web_6.0_HF142 (RO27205)
- Integration_6.0_HF143 (RO27291)
- Client_6.0_HF144 (RO35180)
- Server_6.0_HF145 (RO36446)
- Server_6.0_HF146 (RO41015)

Chapter 8: Known Issues

This section describes the known issues in the current release.

This section contains the following topics:

Tracking ID 221-75: Incorrect Timestamp For Events Captured Immediately Before DST Ends

Events captured in the hour before Daylight Saving Time (DST) ends are stored in the CMS database with an incorrect timestamp. Specifically, CA DataMinder fails to take account of clocks being adjusted backward at the end of DST, so events captured in the preceding hour are stored with a timestamp that is +1:00 hour later than it should be. In the worst case, the iConsole may report events as being captured in the wrong order. For example, the iConsole may show an email reply as being captured before the original email was sent.

The problem only affects CMSs in time zones that use DST. Also, it can only occur once a year in the 60 minute window before DST ends. Customers are unlikely to experience this anomaly because DST typically ends at a time of low business activity (for example, at 2am on a Sunday).

However, there are plausible conditions under which a customer may experience this problem. For example, consider the following setup:

- A CMS is in San Francisco, where Pacific Daylight Time (PDT) ends at 2am on 4 November 2012. When PDT ends, San Francisco reverts to 1am Pacific Standard Time (PST).
- CA DataMinder email agents are deployed in Israel and capture two emails on Sunday morning, 4 November. On this date, Israel is on Israel Standard Time (IST). The first email is captured at 10:45 IST. The second email is captured at 11:15 IST.

  But CA DataMinder incorrectly converts the timestamp for the 10:45 email to 09:45 UTC.
- An iConsole reviewer based in Israel reviews the captured emails later in the same week. The iConsole reports the second email as being captured before the first email.

Email	Actual Capture Time	CMS Timestamp	iConsole Timestamp
#1	10:45 IST (01:45 PDT)	09:45 UTC	11:45 IST
#2	11:15 IST (01:15 PST)	09:15 UTC	11:15 IST

In this example, the CMS timestamp for email #1 is incorrect. The correct timestamp, taking account of the clock adjustment at the end of DST, should be 08:45 UTC.

Note: PDT is UTC-07:00. PST is UST-08:00. IST is UTC+02:00.

Tracking ID 397-45: Emails Released From Quarantine Are Not Encrypted

If an email activates a trigger with a quarantine action *plus* a trigger with any action that generates x-headers on the email, the x-headers are not applied when the email is released from quarantine.

For example, if a trigger has an Encrypt action, CA DataMinder normally inserts an 'encryption request' x-header into an unprotected outgoing email. This x-header is then be detected by a third party encryption provider before the email leaves the corporate network. But for emails released from quarantine, the x-header is not inserted and so consequently the email is not encrypted.

Therefore, we recommend that you do not use Quarantine and Encrypt actions together. That is, ensure that policy is configured such that these two actions cannot be invoked by the same email.

Note: This issue does not affect quarantined emails where the 'encryption request' x-header was inserted by a third party encryption provider (for example, the Voltage SecureMail clientless solution, also known as 'SecureMail FlagSecure'). Such emails *are* encrypted when they are released from quarantine.

Tracking ID 417-17: Do Not Include PST Files In Scanning Jobs

We recommend that you do not include .PST files in FSA or CFSA scanning jobs. This is because .PST files can be very large and contain many individual items. This can cause scanning jobs to take a very long time to complete. It can even mean that the .PST contents are not fully analyzed. This can happen if a policy engine takes too long analyzing a .PST file and so exceeds the FSA's permitted analysis timeout. Consequently, the FSA flags the .PST file as a failure.

This recommendation is particularly important for FSA scanning jobs, which do not automatically exclude .PST files. Conversely, CFSA scanning jobs exclude PST files by default (included and excluded files are defined in the Data At Rest Protection folder in the local machine policy).

To apply policy to e-mails and attachments in .PST files, we recommend you run Import Policy jobs, using PSTFile parameters to configure the import job. For details of these parameters, see the *Archive Integration Guide*; search for 'Event Import, parameters'.

Tracking ID 449-72: FSA Incorrectly Reports 'Access Denied' To SharePoint

If you intend to use the FSA to scan items on Microsoft SharePoint sites, the user that the Remote FSA Connector runs as on the SharePoint host machine must have sufficient List and Site permissions to the Microsoft SharePoint site being scanned. For example, a capture-only policy requires at least the 'View Items' and 'View Application Pages' List permissions and the 'Browse Directories' Site permission.

Tracking ID 474-56: Replacement Stub Files For Scanned Office 2007 or 2010 Documents Generate Errors

The FSA and CFSA can move or delete unauthorized files and replace them with explanatory stub files. The content of a stub file is in plain text, but its file name is exactly the same as the original file that it is replacing. Most stub files can be opened by the original application. However, if a Microsoft Office 2007 or 2010 document is replaced with a stub file, it is not possible to open the stub file using Office applications such as Word or PowerPoint. Instead, the user sees an error message such as:

"Word cannot open the file 'report.docx' because the file format or file extension is not valid."

This is because Office 2007 or 2010 applications cannot reconcile the plaintext format of the stub file with the original format of the replaced document. To view the content of the stub file, users must open it using a text editor such as Notepad.

Tracking ID 512-91: Failure To Block HTTP-GET Downloads

Under certain circumstances, CA DataMinder Network can fail to block downloaded documents. This can happen if a user waits one minute or longer before retrying to download a blocked document (for example, by pressing F5 to refresh the Web page).

Why does CA DataMinder Network fail to block the subsequent download attempt? When a user downloads a document from a Web site, CA DataMinder Network tracks the document, passing the document content to a policy engine for analysis but withholding the final segment of the document (technically, the final packet in the data stream) from the user's browser until the policy engine calls back with an instruction to block or allow the download. If the policy engine instructs CA DataMinder Network to block the download, the user's browser sees the connection being reset and informs the user that the document cannot be viewed. However, if the user waits and then retries to download the document, the browser may download just the final segment of the document. If this final segment does not cause a policy trigger to fire, CA DataMinder Network permits it to go to the browser, which can then display the complete document.

Note that CA DataMinder Network is designed to prevent this problem by blocking segments of previously blocked documents, but in each case this information is only cached for one minute. This timeout is necessary in case the document content on the Web server changes so that the document is no longer in breach of policy and does not need to be blocked. However, this method is also reliant on patterns of user behavior whereby a user will retry to download a blocked document as soon as it occurs but is less likely to do so at a later time.

Tracking ID 517-30: Do Not Include NetHood Folders In Scanning Jobs

We recommend that you do not include \NetHood folders in FSA or CFSA scanning jobs. These folders contain links (.LNK files) to remote machines. If the FSA or CFSA tries to scan these links, this can result in Internet connection errors that cause individual processing threads to hang. If the number of links exceeds the number of available threads, the entire scanning job may fail to complete.

Note: By default, \NetHood folders are hidden in Windows Explorer.

Tracking ID 528-99: Boundary Agents Cannot Quarantine Outbound TNEF Emails

Outgoing e-mails containing TNEF data cannot be quarantined if captured by the Milter MTA Agent, IIS SMTP Agent or the NBA. Specifically, this issue affects TNEF encoded e-mails sent to external recipients and which cause an e-mail control trigger to fire.

Note: These CA DataMinder agents are typically used to detect messages entering or leaving an organization (that is, crossing the Internet boundary). This problem does not affect TNEF emails captured by the Exchange server agent or Outlook client agent. TNEF is an email format used by Microsoft Exchange and Outlook.

Tracking ID 534-00: Cannot Block SIP Instant Messages Sent Over UDP

CA DataMinder Network cannot block instant messages sent using an IM application that uses the Session Initiation Protocol (SIP) if the IM application is configured to use UDP instead of TCP.

Tracking ID 540-32: Problem Scanning Unicode Text In Exchange Public Folders

When the FSA scans Exchange Public Folders, it may incorrectly process Unicode text in scanned items if the FSA host server is using 'Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1' as its MAPI client. To avoid this problem, use Outlook 2003 as the MAPI client on the FSA host server.

Tracking ID 557-92: CFSA Can Prevent BitLocker From Encrypting Removable Devices

The Client File System Agent (CFSA) can affect the operation of the BitLocker To Go encryption feature on endpoint computers.

If the CFSA is installed on an endpoint computer and configured to apply policy to files being copied to removable devices (such as USB drives or SD cards), BitLocker cannot initialize removable devices for encryption. That is, it cannot give these devices the "lockdown treatment". This is because the BitLocker initialization process is denied write access to the device by the CFSA.

Note: This problem only occurs if the CFSA is explicitly configured to apply policy to removable devices. Also, if a removable device has been initialized by BitLocker running on a different computer, the device can used on any endpoint computer hosting the CFSA, even if the CFSA is configured to apply policy to removable devices.

Tracking ID 571-43: Performance Problems on SQL Server CMSs

Under certain circumstances on SQL Server CMSs we have observed performance problems when running iConsole searches and reports. For example, users assigned to a Self-Exclude security model are more likely to suffer from this issue.

This issue is caused by a known problem in SQL Server that can occur when:

- A database query contains at least one JOIN clause.
- There are multiple columns in the WHERE clause.
- The SQL Server optimizer uses the ANTI SEMI JOIN operator to join data (this is a NOT EXISTS sub query)

DBAs can verify whether a CMS is suffering from this problem by analyzing a SHOW STATISTICS PROFILE query plan for the slow running query. Indicative symptoms are:

- Elements of the query plan show a large divergence between the Actual Row Count (showing the correct value) and the Estimated Row Count (highly underestimated; possibly estimated at one).
- Divergent row count estimates originate from an ANTI SEMI JOIN operator row.

In this situation, we recommend that you apply the fix described in Microsoft Knowledge Base article 2222998.

Tracking ID 574-69: Incident Dashboard Does Not Support Non-UTF Databases

CA recommend the following Oracle database versions for use with CA DataMinder:

- Oracle 10g (10.2.0.4 or later)
- Oracle 11gR1 (11.1.0.7 or later)
- Oracle 11gR2 (11.2.0.1)

With earlier versions of Oracle 10g (such as 10.2.0.1 and 10.2.0.3), the Incident Dashboard can produce compilation errors if the database is configured with the default character set (where NLS_CHARACTERSET = <WE8MSWIN1252>).

The workaround for this problem is to configure the database to use a UTF-8 character set before installing CA DataMinder.

Tracking ID 576-13: Notes Agent Fails for Multi-Users Already Using Lotus Notes

(Windows Vista and Windows 7 only; multi-user Notes installations only)

After installing the CA DataMinder Notes agent on a Windows Vista and Windows 7 client machine hosting a Notes multi-user installation, the agent fails to detect emails sent or received by any users who were already using Notes on the client machine before the agent was installed. The workaround is to edit the individual user's notes.ini configuration file

To edit notes.ini

1. Find notes.in in the user's application data folder. For example:

   C:\Users\FrankSchaeffer\AppData\Local\Lotus\Notes\Data

   Note: A user's \AppData\Local folder may be hidden. Change the view options of the parent folder to make hidden folders visible.

2. In notes.ini, locate the EXTMGR_ADDINS line in the [Notes] section.

   If the line does not exist, add:

   ```
   EXTMGR_ADDINS=wgnemno.dll
   ```

   If the line does exist, then add 'wgnemno.dll' to the existing list using a comma separator. For example:

   ```
   EXTMGR_ADDINS=logdll,amgrdll,wgnemno.dll
   ```

3. Restart Lotus Notes for the change to take effect.

Note: This problem only affects 'already-active' Notes users. If a user has not used Notes on the client machine before the Notes agent is installed, the agent *will* successfully detect their emails when they start using Notes after the agent has been installed. In addition,, single user Notes installations and Notes users on Windows XP machines are wholly unaffected.

Tracking ID 576-17: Which Versions of Outlook Does the Quarantine Manager Need to Release Exchange Emails?

To release Exchange or Outlook emails from quarantine, Quarantine Manager uses an Exchange mailbox to forward the emails to their intended recipients. At the same time, Microsoft Outlook must be installed on the Quarantine Manager host machine. However, the required version of Outlook depends on which version of Exchange is being used to host the Quarantine Manager mailbox. If the mailbox is hosted on:

- Exchange Server 2010, then Outlook 2007 or 2010 must be installed on the Quarantine Manager host machine.
- Exchange Server 2003 or 2007, then Outlook 2003 or later must be installed on the Quarantine Manager host machine.

Tracking ID 579-97: DMC Cannot Export to PST Using Outlook 2010 (64-bit)

It is not possible to export e-mails to PST files from the Data Management Console (DMC) if Outlook 2010 (64-bit) is the default e-mail application on the DMC host machine. This is because the DMC runs as a 32-bit process and requires 32-bit MAPI. However, Outlook 2010 (64-bit) uses 64-bit MAPI.

Tracking ID 580-99: Cannot Analyze Fingerprinted Documents Being Printed

Content agents cannot reliably detect fingerprinted files sent to a printer. These are protected files whose content has been registered by CA DataMinder. Consequently, we advise that you do not use Data In Motion content agent triggers to prevent users from printing these documents.

Tracking ID 582-51: 'Replace Email' Control Actions Not Supported for Outlook 2010 or Later

On CA DataMinder client machines hosting Outlook 2010 or later, the Replace action for an incoming email can sometimes fail. That is, the email's original content will still be visible to the recipient. The cause of this problem is currently unknown. Note also that the alternative Delete action does work.

Note: You specify that an incoming email is replaced or deleted by configuring the Delete or Replace? setting in the user policy. This setting is included in the control actions for incoming emails.

Tracking ID 583-37: FSA Logfile Misrepresents Failure To Analyze Text Content

If a policy engine is unable to extract the text content of a file for analysis, the FSA fails to log this as an error. Instead, it only reports an informational log entry (code I2E19). This code is normally used to identify files that were analyzed by CA DataMinder but where no trigger fired, either because the file was benign or because it was on an Excluded List or Ignored List in the user policy.

Note: There can be several reasons why a policy engine fails to extract a file's content. For example, the document may be encrypted or the file type may be unrecognized.

Tracking ID 585-38: MSN Instant Messages Incorrectly Saved As Network Events

If the MSN Instant Message client program, Windows Live Messenger, sends instant messages tunneled through HTTP instead of using the MSN Messenger protocol directly (typically because a firewall is blocking the usual ports), CA DataMinder Network interprets sent messages and any attached files as HTTP-POST documents. The filename given to these captured HTTP-POST documents will always be gateway.dll. Consequently, Windows Live Messenger activity captured by CA DataMinder Network is stored on the CMS as network events, rather than IM events. Any iConsole searches for IM events must take this into account.

Tracking ID 586-31: Encrypt Action Fails For Files Copied From Remote Server To Workstation Using RDC

The Client File System Agent (CFSA) may fail to apply Advise Encrypt or Enforce Encrypt control actions to files copied between machines using Remote Desktop Connection (RDC).

This problem typically affects users connecting via RDC to a remote server from their workstation. Under RDC, in Windows Explorer it is possible to expose any drive on the workstation as a network drive on the remote server. This enables users to copy files from the server directly to their workstation. However, the CFSA is unable to encrypt these file copy operations, though it can apply other control actions such as Block or Warn.

Tracking ID 586-36: Application Agent May Not Apply Policy If User Account Control (UAC) Enabled

If User Account Control (UAC) is enabled on a machine with Windows Vista or later, the CA DataMinder Application Agent, by default, can only apply policy to elevated applications; it cannot apply policy to non-elevated applications.

However, restarting the Application Agent host machine after installation enables the agent to apply policy to non-elevated processes, but not to elevated processes (the Application Agent cannot concurrently monitor elevated and non- elevated applications).

Tracking ID 595-91: Compliance Audit Report Can Show Inconsistent Eligible Event Counts

The results page of the Compliance Audit Report shows an Eligible column. This shows the total number of events that a reviewer is permitted to review. However, values in this column can differ, depending on who runs the report and whether a 'self-exclude' security model is assigned to a reviewer featured in the report.

Example

Consider two reviewers, Reviewer A and Reviewer B, where Reviewer B is assigned to the Policy (Self-Exclude) security model.

When Reviewer A runs this report, the Eligible column shows 100 events for Reviewer B. This incorrectly includes 5 events in which Reviewer B was himself a participant. This is a known error in the software.

But when Reviewer B runs this report, the Eligible column correctly shows 95 events for Reviewer B. This is because Reviewer B's security model prevents him from reviewing events in which he himself was a participant, and so these 5 events are accordingly excluded from the Eligible events count.

Tracking ID 595-00: Policy Engine Fails to Analyze Large .Jar and .Zip Files

Policy engines (PEs) can sometimes fail to analyze archives of .jar files or very large .zip files. This is because these items expand in memory and can consume all of a PE's available memory resources. This problem mainly arises when using the FSA to scan many of these files in parallel.

If you experience excessive memory consumption by a PE, we recommend that you reduce the maximum number of concurrent operations, ideally to one or two and at most to the number of physical CPU cores in the PE host server. To do this, you must edit the machine policy for the host server. Specifically, you need to edit the Maximum Number of Concurrent Operations setting; find this in the Policy Engine folder.

Tracking ID 597-54: Custom Search and Report Upgrade Issues

(Only applies to searches and reports created in CA DataMinder versions 6.0 or 12.0)

The current CA DataMinder release includes essential changes to the iConsole to improve accessibility and usability. However, these changes mean that some 6.0 or 12.0 custom searches and reports may cause JavaScript errors when a user views the customization or results pages for such searches and reports.

As an alternative to fixing your 6.0 or 12.0 custom searches and reports, we recommend that you review the standard searches and reports that ship with CA DataMinder. You may find that these now adequately meet your needs. The Standard Reports package contains 16 reports covering compliance, incidents and issues. It also contains six standard searches. For details about these, see the 'iConsole Standard Searches, Reports and Policies' chapter in the *Platform Deployment Guide*.

If replacing a custom search or report with a standard one is not viable, you will need to modify the XML search definition files for any affected search or report to fix the JavaScript errors. Details of the required compatibility changes are in the 'Changes to Javascript for Custom Reports and Searches' chapter in the *iConsole Search Definition Reference Guide*.

Note: A custom search or report is one produced by Orchestria or CA for a specific customer, or one developed by the customer themselves.

Tracking ID 630-92 Data in Motion Limitation for Notepad Files

The Client File System Agent (CFSA) is typically used to apply policy to files copied to removable USB devices, network locations, and sync folders using Windows Explorer. However, if users edit files directly on USB devices or in sync folders using Notepad or Wordpad, the CFSA may inadvertently delete the file.

This problem occurs if a user uses Notepad or Wordpad to edit a file saved on a USB device or in a sync folder *and* adds some prohibited text to that file. When the user clicks Save, CA DataMinder displays a Warning dialog and deletes the file. Consequently, the only remaining copy of the file is the one currently displayed in the Notepad or Wordpad window. If the user closes Notepad or Wordpad, the standard Window dialog appears ('Do you want to save the changes?'). Now, regardless of whether the user clicks Yes or No, the dialog closes and the text content is lost completely.

To avoid this problem, we recommend that users always edit their files on a fixed disc and then copy them to a USB device or sync folder.

Tracking ID 619-20: First File Copied by Command Line is not Encrypted

If the CFSA is configured to apply user policy and you set a Data In Motion control action to 'Force Encryption', you can force users to encrypt files being copied to removable devices.

However, if the user copies the file to a removable device from a command line, the encryption fails. This problem only occurs on the first copy operation of the command line session. If the user copies a second file (or copies the same file again) in the same command line session, the CFSA successfully encrypts the file.

Note: If a user runs a batch file to copy multiple files, the encryption failure affects each file.

Tracking ID 644-72: Installation time-outs on Oracle CMSs

Under certain conditions, an installation process times out when you install CA DataMinder components into an existing Oracle database on the CMS or a gateway server. When a time-out occurs, you see this error message:

```
ORA-04021: timeout occurred while waiting to lock object
```

This message indicates that a database object is locked by a separate database process. Consequently, the installation process cannot update or remove the object. The following list contains examples of database processes which, if running, can lock objects required by the installation process:

- iConsole searches or reports, including BusinessObjects reports for CA DataMinder
- Data warehousing jobs
- Database statistics collection, especially processes that call the CA DataMinder wgn_stats package
- Data ingestion processes. For example, CA DataMinder email agents, archive agents, and Event Import jobs, can conflict with the installation process when they write events into the CMS database
- DBAs running SQL Statements in SQL*Plus or SQL Developer, or in third-party tools such as SQL Navigator or TOAD
- Database purges, including infrastructure-based purges and partition-based purges

Where possible, we recommend that you allow these processes to complete before you retry the installation.

Alternatively, if there is no risk of data loss, you can terminate the locking process. For example, if you terminate a process that only queries the database (such as reports and searches), there is a low risk of data loss. Conversely, if you terminate a process that updates the database (such as data ingestion), the risk of data loss is considerably higher.

When the locking process has completed or been terminated, you can retry the installation.

Tracking ID 648-01: Reviewer Activity Report Misrepresents Individually Audited Events

Under certain conditions, the BusinessObjects versions of the Reviewer Activity and Compliance Audit reports show wrong event totals in the Individual Audited and Bulk Audited columns.

The report shows the activity of individual reviewers in terms of the number of events viewed and audited. In particular, it shows how many individual events a reviewer has audited, and how many events they have updated in bulk audits.

However, if a reviewer performs a bulk audit on a set of events and also audits one of these events individually, the report fails to add this event to the Individual Audited column. Instead, the event is included in the Bulk Audited column.

Note: This problem only affects the BusinessObjects versions of the Reviewer Activity and Compliance Audit reports. This problem does not affect the standard CA DataMinder Reviewer Activity and Compliance Audit reports.

Tracking ID 674-14: SideBySide Errors Logged on 64-bit Policy Engines

When a policy engine on a 64-bit server analyzes events, SideBySide errors are sometimes written to the Windows application log.

These error messages are generated by the third-party component, libeay32.dll. CA DataMinder uses this component to extract text content from captured or imported events.

To prevent these SideBySide error messages, install the Microsoft Visual C++ 2008 Redistributable Package (x64) on the policy engine host server. You can download this package from:

http://www.microsoft.com/en-us/download/details.aspx?id=15336

Tracking ID 674-50: Oracle Data Warehousing Job Fails with ORA-07445 Error

A data warehousing job may fail on Oracle 10GR2 (any 10.2 variant) with Oracle error: `ORA-07445: exception encountered: core dump [ACCESS_VIOLATION] [qessoCanNewSort+554]`

This is Oracle Bug 5854471. If you see this error, ask Oracle Support if a patch is available for your version of the Oracle database server. Apply the patch if available. Alternatively, consider upgrading your Oracle database to 11G.

Apply the workaround

If neither of these options is possible, you can manually apply workaround suggested by Oracle Support in Bug 5854471. For this workaround, you must edit the data warehousing job command:

1. Use Oracle Enterprise Manager to locate scheduler job named DLP_AGGREGATION_<dbname>.
2. Edit the command as shown in the following example:

   Before editing the command

   ```
   BEGIN dlp_agg.rut_dlp_aggregation_process( BDEBUG => 1 );
   COMMIT;
   END;
   ```

   After editing the command

   ```
   BEGIN EXECUTE IMMEDIATE 'alter session set "_newsort_enabled"=false';
   dlp_agg.rut_dlp_aggregation_process( BDEBUG => 1 );
   COMMIT;
   END;
   ```

   Important! Do not change the BDEBUG argument value!
3. Save the change.

Important! You must undo this change if you later upgrade your Oracle database to version 11 or later.

Tracking ID 679-44: Exchange 2013 Server Agent Fails to Apply Policy to Incoming Sent-to-Self Emails

To handle a known issue in Exchange 2013, the Outlook endpoint agent has been modified. However, this modification to the agent impacts CA DataMinder handling of incoming send-to-self emails.

If a user sends an email to themself (for example, to test that CA DataMinder policy triggers are operating as intended), the Outlook endpoint correctly applies policy to the *outgoing* email when it is sent. But it fails to apply policy to the *incoming* email when it arrives in the user's inbox.

This issue only affects incoming send-to-self emails. It does not affect incoming emails from other senders.

Note: The known issue in Exchange 2013 occurs when Outlook uses an email profile configured for an Exchange account, but the mailbox for that account resides on an Exchange 2013 server. In this situation, sent emails have the attributes of *received* emails. To accommodate this error, and to prevent CA DataMinder from applying incoming email triggers when a user opens an email in their Sent Items folder, the Outlook endpoint agent uses a modified method to detect *genuine* incoming emails. But as a consequence, the Outlook agent can no longer detect and apply policy to incoming send-to-self emails.

Tracking ID 682-55: CPSA Cannot Apply Policy to Documents Printed with Windows 8 XPS

Microsoft have introduced a new print processing system in Windows 8, known as XPS (XML Paper Specification) printing. This new system is in addition to the legacy GDI printing system.

In the current CA DataMinder release, the Client Print System Agent (CPSA) is unable to analyze documents printed using the XPS system. This limitation includes documents printed from Metro applications and Internet Explorer. Consequently, Data In Motion triggers are not applied to documents printed using the Windows 8 XPS printing system. This feature will be addressed in a future release.

Tracking ID 683-99: Office Files Copied from SharePoint by FSA Are Not Smart Tagged

You can configure Data At Rest triggers to add smart tags to scanned files. However, if the File Scanning Agent (FSA) copies a scanned Microsoft Office file from a SharePoint library to the file system, smart tags do not get added to the copied file.

Note that this problem does not affect Office files copied from a file system. If the FSA copies these files to a new location, they are smart tagged correctly.

Tracking ID 686-07: EMC SourceOne 6.8.2 Not Supported

CA DataMinder does not support EMC SourceOne 6.8.2 due to incompatible product changes introduced in this version.

Tracking ID 687-32: CFSA Deletes Existing File if Overwrite Operation is Blocked

The Client File System Agent (CFSA) is typically used to apply policy to files copied to removable devices or network locations using Windows Explorer.

However, if a user tries to overwrite an existing file with a new version that contains prohibited text, the CFSA correctly blocks the new version from being copied. But the blocking mechanism also deletes the existing file.

For example, a manager copies a weekly status report from their workstation to a network folder monitored by the CFSA. The CFSA analyzes the report and detects no problems. It therefore allows the report to be copied. Later in the week, the manager updates the report on their workstation with new details about a sensitive project. Now when the manager tries to copy the updated report to the network folder, the CFSA blocks the operation. However, it also deletes the original version of the report in the network folder. Consequently, the only remaining copy of the file is the updated version on the manager's workstation.

Tracking ID 692-39: Unable to Open Dashboard Incident Tables in New Window in IE8

For iConsole dashboards running in Internet Explorer 8, a JavaScript error occurs when a reviewer clicks the Open in a New Window button for the 'grid' charts, Incidents By Policy and Incidents By Sender.

To avoid this problem run the dashboard in Internet Explorer 9 or 10, Google Chrome, or Mozilla Firefox.

Note: This problem only affects the two grid charts mentioned above, and only occurs in Internet Explorer 8 browsers.

Tracking ID 692-86: Unable to De-duplicate Multiple SMTP Emails Generated by Voltage SecureMail ZDM Web Application

If a user sends an email to multiple recipients using the Voltage Zero Download Manager, a separate copy of the SMTP email is generated for each recipient. CA DataMinder processes each copy separately, resulting in multiple email events on the CMS for what appears to be a single email.

Issues can also arise if CA DataMinder quarantines these emails. Depending on which agent captured the original email, reviewers may need to release each copy of the email separately from quarantine. If the emails were originally captured by the Exchange server agent, CA DataMinder forwards all copies of the emails to their respective recipients when a reviewer releases *just one copy* (addressed to a single recipient) from quarantine. But if the emails were originally captured by the Milter MTA agent or IIS SMTP agent, CA DataMinder only forwards the copy that was directly released from quarantine.

For example, an email is sent to Spencer Rimmel and Frank Schaeffer, resulting in two copies of the same email. CA DataMinder quarantines both copies. A reviewer subsequently releases from quarantine the copy addressed to Spencer Rimmel.

- If the original email was captured by the Exchange server agent, the copies to both Spencer Rimmel and Frank Schaeffer are forwarded simultaneously.
- If the original email was captured by the Milter MTA agent or IIS SMTP agent, only the copy addressed to Spencer Rimmel is forwarded. The copy addressed to Frank Schaeffer remains quarantined and must be released separately.

Tracking ID 693-54: CFSA Can Incorrectly Deny Drag-and-Drop onto Dropbox Shortcut

Occasionally and only under specific conditions, the Client File System Agent (CFSA) incorrectly blocks a DropBox drag-and-drop operation. This can happen when a user drops a file onto the DropBox shortcut on their desktop.

Normally, DropBox starts automatically and runs as a background instance when a user logs on. If the user drags a file onto the DropBox shortcut, a new instance of DropBox starts. The new instance runs long enough to sync the file with the DropBox web server and then stops.

However, if the background instance of DropBox is not running, the new DropBox instance continues running after the file has been synced. The CFSA is unable to interact correctly with the still-running DropBox instance. As a result, the CFSA allows the initial drag-and-drop operation but blocks any subsequent operations. Specifically, if the user attempts to drag a second file onto the DropBox shortcut, the CFSA denies access to the DropBox sync folder and displays the Access Denied message (as defined in user policy).

The workaround to this problem is to log off. When the user logs off and then logs back on, the correct background instance of DropBox starts and the CFSA correctly handles drag-and-drop operations to the DropBox shortcut.

Note: This CFSA problem can only affect drag-and-drop operations to the DropBox shortcut on the desktop. This problem does *not* affect drag-and-drop operations to the DropBox folder in Windows Explorer or uploads to the DropBox web site.

Tracking ID 694-81: General Limitations of Web Agents

CA DataMinder web agents (Client Network Agent, ICAP agent, and the Network Appliance) have some limitations when attempting to control data submissions from certain sites.

- Some web applications can cause multiple intervention actions to be applied when CA DataMinder detects a policy violation. Typically, this happens with applications that use client-side JavaScript, or technologies such as AJAX to submit data to the web server. CA DataMinder web agents attempt to block such submissions by failing the HTTP request, but if the client-side part of the web application does not handle the failure well, it resubmits the data, resulting in multiple violations.

  Note: The Network Agent attempts to minimize the impact on the user by keeping a history of recent interventions, quietly failing subsequent requests if they appear to be resubmissions and the original was blocked.

- Some web applications, for example Google Docs, upload fragments of data rather than whole files. This can lead to incorrect policy application because if CA DataMinder does not have access to the whole file, it cannot make a correct decision. Consider using policy to block access to such problem sites.

Tracking ID 694-82: Cannot Access HTTPS Sites With Cavium Coprocessor Enabled

Symptom:

Connectivity problems may occur when using the latest browsers (for example, Internet Explorer 10 or Firefox 19) to browse web sites using the SSL protocol (HTTPS). The issue has been observed when the SSL protocol is being decoded by CA DataMinder Network on the Bivio 7000 platform.

Solution:

The workaround is to configure CA DataMinder Network to use software rather than hardware SSL acceleration.

Follow these steps:

1. Create a file that has the name 'disablesslcoprocessor' inside the CA DataMinder Network 'config' folder. The content of the file is not relevant. Use the FTP server or alternatively via the command line and enter the following command:

   ```
   echo > /home/smb/config/disablesslcoprocessor
   ```

2. Restart the unit either by using the web management console and clicking Reboot on the Administration page, or by using the following commands on a shell prompt:

   ```
   nrsp stop nba
   nrsp start nba
   ```

Tracking ID 696-64: iConsole Sometimes Displays Uploaded File Names as UnknownName.dat or BlankName.dat

When uploading files to a web server, some sites use non-standard methods of transmitting the file name, or send it in a web request separate to the uploaded content. The Client Network Agent always attempts to obtain file names, but in some cases will resort to using UnknownName.dat or BlankName.dat - these names can therefore be visible in the iConsole.

Tracking ID 699-20: Intervention Dialogs Not Displayed On Top of Metro Applications in Windows 8

Normally when a CA DataMinder endpoint agent generates an intervention dialog (for example, a blocking notification), the dialog displays on top of the application window that the user was using. For example, if a blocking is triggered when a user tries to send an Outlook email, the dialog displays on top of the Outlook 'compose email' window.

However, under certain conditions in Windows 8, the intervention dialogs display on the desktop and may not be seen by the user. Specifically, if a trigger fires while a user is running a Windows 8 application that uses the new design language (formerly known as ‘Metro’, ‘Modern UI’, or ‘Microsoft design language’) the intervention dialog displays on the Windows desktop. It does not display on top of the application window.

If this happens, the user may fail to notice the intervention dialog. And because the Windows 8 application does not respond until the dialog is cleared, the user may incorrectly assume that the application has stopped working. In such circumstances, we recommend that you advise users to check their Window 8 desktop for relevant notifications.

Note: In practice, the problem is only likely to affect intervention dialogs generated by the Client Network Agent when a user uploads or submits data to a web site using the Windows 8 version of Internet Explorer.

Tracking ID 699-34: Client Network Agent Does Not Analyze IPv6 Traffic on Windows XP and Windows 2003

Due to differences in how IPv6 is implemented in Windows, the Client Network Agent is unable to protect machines using IPv6 if those machines are using Windows XP or Windows 2003. We recommend upgrading to a later version of Windows.

Tracking ID 699-59: Client Network Agent Does Not Analyze Data Submitted from Windows Store Apps

When deployed on Windows 8, the Client Network Agent protects web browsers as usual, but is not able to protect data submissions from Windows Store applications, including the non-desktop version of Internet Explorer. Windows Store applications do not operate as traditional Windows applications and use different means of network communication that are not intercepted by the Network Agent.

Tracking ID 699-70: Blocked Documents Added to Zip Files in Sync Folders Cause Entire Zip File to Be Deleted

The Client File System Agent (CFSA) can delete zip files stored on targets such as removable devices, network folders, or in file sync folders.

If a user attempts to add an unauthorized document to a zip file in a target location monitored by the CFSA, the CFSA blocks the document but also deletes the entire zip file. This happens even if the zip file contains other benign documents that do not breach policy.

If you use the CFSA to protect files copied, we recommend that your users refrain from storing zip files in target locations monitored by the CFSA.

Note: This issue also affects *compressed folders* created in sync folders on Windows 8 and Windows Server 2012 machines. These compressed folders are actually rebadged zip files.

Tracking ID 700-36: CFSA Issues When Using Command Prompt to Move Files into a Sync Folder

The Client File System Agent (CFSA) can apply policy when a user moves files and folders to targets such as removable devices and sync folders using Command Prompt. But the note the following issues:

Windows 7 or earlier

On a system running Windows 7 or earlier, when the user runs a 'move' command to:

- Move *files*, the CFSA actually *copies* the files to the target. This is by design to prevent accidental deletion of the file if CA DataMinder triggers fire.
- Move a *folder*, the CFSA blocks the move operation to prevent a possible data leak (that is, the folder may contain files which are not permitted to be on the target device or sync folder).

  In this case, we recommend that users run a 'copy' command instead of a 'move' command, or that they use Windows Explorer to move the folder.

Windows 8 and Windows Server 2012

On a system running Windows 8 or Windows Server 2012, when the user runs a 'move' command to:

- Move *files*, there is a risk that the CFSA deletes the files.
- Move a *folder*, there is a risk of a data leak. That is, the CFSA permits the folder to be moved even though it may contain files which are not permitted to be ion the target device or sync folder.

In both cases, we recommend that users run a 'copy' command instead of a 'move' command, or that they use Windows Explorer to move the files or folder.

Tracking ID 700-47: New Users May See Certificate Errors in Mozilla or Opera Browsers

Symptom:

If a new user logs on to a machine where the Client Network Agent is installed, the user may see certificate errors when using Mozilla or Opera browsers. The errors occur because the 'CA DataMinder Root' certificate is not automatically trusted by the browser.

Solution:

There are several ways to make the browser trust the certificate.

- The user can manually 'trust' the certificate in Opera or add an exception in Mozilla browsers.
- The user or administrator can restart the machine or the CA DataMinder Policy Engine Service.
- An administrator can install the certificate in the appropriate certificate stores using utilities provided by Mozilla or Opera.

Note: Internet Explorer, Safari, and Google Chrome are not affected by this issue.

Tracking ID 700-97: Incidents By Sender Table Lists Computer Name Instead of User Name in iConsole Dashboard

The Incident Dashboard includes an Incidents By Sender pane. This pane summarizes captured incidents by user. Users names are listed in the Identity column.

However, for Data In Use incidents (Save, Print, and AppMon) and Web incidents captured by CA DataMinder endpoint agents, the Identity column shows the name of the computer hosting the endpoint agent instead of the user name.

This error will be fixed in a future release.

Note: Some incident types, such as incidents captured by CA DataMinder Network, do not have an associated user. For these incidents, the Identity column cannot show a user name. Instead, it shows the name or address of the source server.

Tracking ID 700-99: Drilldown into 'Other Policies' in Dashboard Charts Show Incorrect Incident Count

The Incident Dashboard includes Overall Risk and Incident Trend by Policy charts. By default, these charts show incident counts for the five policies with the highest incident counts, plus an amalgamated incident count for 'Other Policies'. If you drill down into any of these incident counts, you see the underlying incidents.

However, if you drill down into the 'Other Policies', the resulting incidents do not exclude incidents associated with the top five policies. This error will be fixed in a future release.

Tracking ID 701-03: Client Network Agent Incompatible with McAfee MOVE AntiVirus

Do not install the Client Network Agent onto virtual machines which use, or plan to use McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus for virtual desktops. The machine may hang or become unresponsive after installation.

Note: This issue only applies to McAfee MOVE AntiVirus. There are no known issues with other McAfee or other anti-virus products.

Tracking ID 705-19: Anti-Virus Exceptions

We recommend that you exclude the CA DataMinder program (%wgninstalldir%) and data (%wgndatadir%) directories from Anti-Virus checks. This improves performance and ensures that the data is not corrupted by rogue or overly enthusiastic Anti-Virus suites.

Tracking ID 706-10: Incident Details Missing From iConsole Event View Page

When CMS and Policy Engine are not installed on the same physical machine, incident information data is missing from iConsole event view page.

Symptom:

When CMS and PE Server are installed on two different machines, policies are getting triggered at ICC level, and events are captured in the iConsole.

But the details of policy are blank in the right-hand-side pane of the event in the iConsole, and I cannot see the event under 'Recent Incidents'. I have to go to 'Standard Search' to view the event.

Solution:

Install CMS and PE together on same machine. Then you can see the details of triggers in the iConsole, and the events appear under 'Recent Incidents'.

Tracking ID 706-11: Smart Tag Name Cannot Have Multiple Values

The CA DataMinder Integration Agent does not support multiple values for single Smart Tag names.

Symptom:

If I use multiple values for a single smart tag name in multiple policies, then, depending on the order of policy triggers, the smart tag values are overwritten. The smart tag value finally holds the last value of the last policy that was triggered.

Solution:

Create a separate smart tag name in the ICC for each smart tag value.

Appendix A: Third Party Service Acknowledgements

CA DataMinder incorporates software from third–party companies. License agreements are available in the \Bookshelf Files\TPSA folder in the CA DataMinder bookshelf. They are listed in the following file:

third_party_software_acknowledgments.txt