

# CA DataMinder

## Upgrade Guide

Release 14.6



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

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

# 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](mailto: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

---

<b>Chapter 1: Upgrading CA DataMinder</b>	<b>7</b>
<b>Chapter 2: Version, Policy and File Compatibility</b>	<b>9</b>
CMS .....	9
Client Machines .....	10
iConsole Servers .....	10
Event Files and Search Files.....	10
Policy Transfers .....	11
Custom Base Policies.....	12
<b>Chapter 3: Pre-Upgrade Tasks</b>	<b>13</b>
Migrate Registry Values .....	13
Back Up and Suspend the CMS .....	14
Upgrade .NET Framework on iConsole Servers.....	15
<b>Chapter 4: Upgrade Procedures</b>	<b>17</b>
Recommended Upgrade Sequence.....	17
How to Upgrade a CA DataMinder Computer.....	18
Upgrading the CMS .....	18
Upgrading Policy Engines on 64-bit Systems.....	19
Upgrading iConsole Servers .....	20
Will My Custom Searches Still Run?.....	21
Do I Need To Delete Temporary Internet Files After Upgrading?.....	21
Upgrading the Universal Adapter.....	22
<b>Chapter 5: Upgrading from 14.1</b>	<b>23</b>
Upgrade CA Business Intelligence 3.2 to 3.3.....	23
Replace Web Triggers with Web-Targeted Data In Motion Triggers .....	25
<b>Chapter 6: Upgrading from 14.0</b>	<b>27</b>
Change in 'Data In Use' Behavior for Client File System Agent (CFSA).....	27
Automatically Reassign Users with Custom Roles to Equivalent 'Official' Roles.....	28
Replace Web Triggers with Web-Targeted Data In Motion Triggers .....	30
Enable BusinessObjects Reports for CA DataMinder .....	31

---

## Chapter 7: Upgrading from 12.5 33

Dashboards .....	33
Delay Before the Dashboard is Updated .....	34
Historical Dashboard Data is Lost After Upgrade .....	35
Change in 'Data In Use' Behavior for Client File System Agent (CFSA) .....	36
Automatically Reassign Users with Custom Roles to Equivalent 'Official' Roles .....	37
Replace Web Triggers with Web-Targeted Data In Motion Triggers .....	39
Change in AuthenticatedUserType Default Value for ICAP Agent .....	40
Color Coding for Incident Rate By Policy Report .....	40

## Chapter 8: Upgrading Databases 41

Database Schema Changes .....	41
Pre-upgrade Database Considerations .....	41
Back Up Your CMS Database Before Upgrading .....	41
Oracle Issues .....	42
Upgrading a Partitioned Oracle Database .....	42
Semi-automated Database Upgrades .....	42
Native Upgrade Scripts .....	45
Native Script Upgrades from r12.5 .....	47
Native Script Upgrades from 14.0 .....	48
Native Script Upgrades from 14.1 .....	49
Native Script Upgrades from 14.5 .....	50
Upgrading the Data Warehouse .....	51
Run a Native Script to Upgrade the Data Warehouse .....	52
Partition the New Data Warehouse Tables .....	54
Retrospectively Enable a Data Warehouse After Upgrading .....	54
Set Credentials for the Reporting User .....	55
Set Credentials for the Unrestricted Search User .....	56
Enable the Data Warehouse After Installing .....	57
Configure Support for BusinessObjects Reports .....	58
Performance Enhancements for Searches and Reports .....	58
Stored procedure: wgn_queryflags_migrate .....	59

## Index 63

# Chapter 1: Upgrading CA DataMinder

---

This guide describes how to upgrade previous CA DataMinder deployments to CA DataMinder 14.6. It highlights the essential issues you need to be aware of when rolling out upgrades across your organization and describes any necessary post-upgrade tasks.

**Note:** This guide does not cover upgrades from earlier versions than CA DLP 12.5. If you want to upgrade from earlier versions, contact [Technical Support](#).



# Chapter 2: Version, Policy and File Compatibility

---

Upgrading individual CA DataMinder machines is simple. In principle, we recommend that you upgrade all your CA DataMinder servers (gateways, Event Import machines, policy engines, and so on) at the same time as the CMS. Do this during a period of minimal user activity, beginning with the CMS and then working down the machine hierarchy to each server successively.

In practice, we recognize that this is not always possible. In very large organizations, the upgrade rollout can easily take several weeks. Likewise, unforeseen complications may force you to upgrade child machines before their parent server has been upgraded.

For these reasons, you will inevitably have different version machines operating alongside each other during the upgrade rollout. Any compatibility issues involved with running a new CMS with older versions of other components (for example, the Administration console or Data Management console), are covered in their own sections.

Before starting the rollout, you need to understand how CA DataMinder handles data transfers (policy changes and captured data) between machines running different versions of the product.

**Note:** CA DataMinder does not support different versions of the product running on the same machine.

This section contains the following topics:

[CMS](#) (see page 9)

[Client Machines](#) (see page 10)

[iConsole Servers](#) (see page 10)

[Event Files and Search Files](#) (see page 10)

[Policy Transfers](#) (see page 11)

[Custom Base Policies](#) (see page 12)

## CMS

There are no known issues connecting an upgraded CMS to earlier version CA DataMinder components, with the exception of the [iConsole](#) (see page 10).

In particular, there is no risk of data loss due to upgrading. Events captured on non-upgraded machines are replicated up to upgraded parent servers as normal.

## Client Machines

If necessary, you can upgrade your endpoint agents after upgrading your gateway servers.

## iConsole Servers

Be aware of the following issues:

### **iConsole servers and CMS must be same version**

We do not support mixed version deployments. You must upgrade your CMS, iConsole application servers and front-end Web servers together. If the CMS and iConsole servers are running different versions of CA DataMinder, the iConsole may not function correctly

For example, we do not support upgraded iConsole servers connected to an older version CMS. Likewise, we do not support older version iConsole servers connected to an upgraded CMS.

We recommend that you upgrade the CMS first, then the application server, followed immediately by your front-end Web servers.

### **iConsole searches and reports**

After upgrading your CMS, you will be unable to run searches or reports in the iConsole until it too is upgraded.

### **iConsole policies**

After upgrading your CMS, you will be unable to edit policies in the iConsole until it too is upgraded.

## Event Files and Search Files

The current version of CA DataMinder supports EVF, EVL, EVS and QDF files generated by all earlier versions of CA DataMinder.

## Policy Transfers

Following a CA DataMinder upgrade, policy compatibility between servers and client machines running different versions of CA DataMinder depends on two factors: whether the upgrade involved a major or minor change in the version of the policy schema, and whether the parent server was upgraded before or after its child machines.

Upgrades to the current CA DataMinder version involve a minor change in the schema versions for both machine policy and user policy. A minor version change implies that the policy structure has not changed, but that some additional policy settings have been introduced.

### **Parent server upgraded first**

Policy changes are transferred from upgraded parent servers down to non-upgraded child machines, but any new policy settings (that is, settings not present in existing policies on the child machine) are simply ignored by the child machine.

### **Child machine upgraded first**

Upgraded child machines cannot operate with non-upgraded parent servers. Policy changes are not transferred from non-upgraded parent servers down to upgraded child machines.

## Custom Base Policies

If you have a custom base policy (that is, a user policy with additional triggers and/or document classifications), this requires careful handling during the upgrade process.

With each new CA DataMinder release, the number of available triggers and document classifications typically increases.

### To upgrade a custom base policy

1. Check whether the base policy on an upgraded CMS has enough triggers and/or document classifications to satisfy your needs.

See the following section for trigger and document classification counts.

2. If the base policy on an upgraded CMS has sufficient triggers and/or classifications, no special upgrade steps are necessary.

When you upgrade your CMS and gateway servers, your custom base policy is automatically supported on these machines.

3. If the base policy on an upgraded CMS still does not have sufficient triggers and/or classifications, you must apply to CA for updated versions of the base policies that also include your customizations. To do this:

- a. Contact [CA Technical Support](#).
- b. After you have received these updated base policies, carry out your CA DataMinder upgrade.
- c. You then need to apply the updated base policies.

**Note:** We strongly recommend you apply for updated base policies before upgrading.

# Chapter 3: Pre-Upgrade Tasks

---

This section describes pre-upgrade tasks that you must perform before upgrading certain components.

**Note:** See also the pre-upgrade database considerations in the 'Upgrading Databases' chapter.

This section contains the following topics:

[Migrate Registry Values](#) (see page 13)

[Back Up and Suspend the CMS](#) (see page 14)

[Upgrade .NET Framework on iConsole Servers](#) (see page 15)

## Migrate Registry Values

Before you upgrade CA DataMinder, you may need to migrate the existing product registry keys.

### Product Registry Key Has Been Renamed

CA Technologies is renaming its security portfolio to follow the Minder product family. In particular, CA DLP has been renamed to CA DataMinder in the current release. In parallel with this product name change, the registry key used by CA DataMinder components has also been renamed.

- In Orchestria APM 6.0, the product registry key was:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Orchestria\Active Policy Management
- In CA DLP 12.0, 12.5 and 14.0, the product registry key was:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\CA DLP
- In 14.1 and later, the product registry key is:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\ComputerAssociates\CA DataMinder

### **Do I Need to Manually Migrate Existing Registry Keys?**

If you upgrade any pre-14.1 CA DataMinder computer by running setup.exe, the CA DataMinder installation wizard automatically migrates the existing product registry key to the new CA DataMinder registry key.

However, if you plan to upgrade CA DataMinder by running an .msi installer package directly (for example, server.msi or integration.msi), you must migrate the registry key manually *before you upgrade CA DataMinder!*

Specifically, before you upgrade any CA DataMinder server (including the CMS), endpoint computer or utility machine, use the migreg.exe utility to copy existing registry values to the new 'CA DataMinder' registry key. The upgrade is blocked if CA DataMinder detects that registry values have not been migrated to the new key.

### **To manually migrate existing registry keys**

1. Find migreg.exe in the \Support folder on your CA DataMinder distribution media. We recommend that you copy this utility to a suitable network location.
2. Before you upgrade a CA DataMinder computer, run this command locally:

```
<path>\migreg
```

Where <path> specifies the migreg.exe location you chose in step 1.

3. (Optional) After successfully upgrading all CA DataMinder components on a computer, run this command to purge the old Orchestria or CA DLP registry keys:

```
<path>\migreg -p
```

## **Back Up and Suspend the CMS**

We recommend that you back up and suspend your CMS before upgrading:

### **Back up the CMS**

For details, see the *Platform Deployment Guide*; search for 'CMS, backing up'.

### **Suspend the CMS**

Manually suspend the CMS before upgrading.

Do this in the Administration console (see the online help for details; search for 'CMS, suspend').

Alternatively, run the following command from the \system subfolder in the CA DataMinder installation folder on the CMS:

```
wgninfra -exec wigan/infrastruct/Infrastruct Suspend
```

## Upgrade .NET Framework on iConsole Servers

For the current version of CA DataMinder, your iConsole host servers must be running:

.NET Framework 2.0

If necessary, you must upgrade the currently installed version of ASP.NET before upgrading your iConsole servers. The upgrade will fail if the host machine is not running .NET Framework 2.0.



# Chapter 4: Upgrade Procedures

---

This section contains the following topics:

- [Recommended Upgrade Sequence](#) (see page 17)
- [How to Upgrade a CA DataMinder Computer](#) (see page 18)
- [Upgrading the CMS](#) (see page 18)
- [Upgrading Policy Engines on 64-bit Systems](#) (see page 19)
- [Upgrading iConsole Servers](#) (see page 20)
- [Upgrading the Universal Adapter](#) (see page 22)

## Recommended Upgrade Sequence

We recommend that you systematically work down the machine hierarchy, upgrading each parent server before you upgrade its child machines. This will minimize disruption to users, and prevent possible loss of policy changes.

To upgrade CA DataMinder

1. (Only required if upgrading from version 6.0) Migrate the old Orchestria registry keys.
2. Upgrade and then restart the CMS.

**Note:** After upgrading your CMS, you will be unable to run searches or reports in the iConsole until it too is upgraded.

3. Upgrade and then restart the following CA DataMinder servers:
  - Gateways
  - Policy engines
  - Event import machines
  - Remote Data Manager machines
  - Quarantine Manager machines
4. Upgrade your iConsole servers and the standard iConsole searches and reports.
5. Upgrade your email server agents, including:
  - Exchange server agent
  - Domino server agent
  - Milter MTA agent
  - IIS SMTP agent

6. Upgrade other CA DataMinder components, including:

- Integration agents
- File scanning agent jobs
- Universal Adapter

7. Upgrade and then restart your client machines

If you plan to upgrade your client machines using a managed deployment method such as Group Policy, you **must** manually upgrade the parent gateway before upgrading the client machines.

**Note:** For details on Group Policy deployments, see the *Endpoint Integration Guide*; search for 'client machines, installation, Group Policy'.

## How to Upgrade a CA DataMinder Computer

All CA DataMinder upgrades can be run using a single executable. CA DataMinder automatically detects that you are upgrading and launches the appropriate installation wizard.

**Follow these steps:**

1. Run setup.exe on each 64-bit host computer.

Run setup32.exe on each 32-bit host computer.

Find these files in the root of the CA DataMinder distribution image.

2. The CA DataMinder server installation wizard starts.

The wizard automatically detects that you are upgrading. You do not need to supply any further details.

3. Proceed to the final screen and install the upgrade.

4. When the upgrade completes, restart the computer.

## Upgrading the CMS

When upgrading your CMS, note the issues below.

**Back up your database!**

Before you upgrade your CMS, back up your CMS database.

**Database user accounts**

If upgrading an Oracle CMS, new Oracle user privileges may be required.

## Upgrading Policy Engines on 64-bit Systems

By default, the installation wizard installs a 64-bit policy engine when you upgrade an existing policy engine on a 64-bit system.

However, version 12.5 and 14.0 policy engine hubs are 32-bit components and cannot connect to 64-bit policy engines. If you must retain and use 12.5 or 14.0 policy engine hubs in conjunction with upgraded 64-bit policy engines, you must apply the following patches to your 12.5 and 14.0 policy engine hubs (or Remote Policy Engine Connectors):

- For a 12.5 policy engine hub running on a 32-bit server, apply this hotfix:  
integration\_12.5\_HF0172 (RO55146)
- For a 12.5 policy engine hub running on a 64-bit server, apply this hotfix:  
integration\_x64\_12.5\_HF0173 (RO55146)
- For a 12.5 Remote Policy Engine Connector, apply this hotfix:  
server\_12.5\_HF0174 (RO55146)
- For a 14.0 policy engine hub on a 32-bit server, apply this hotfix  
integration\_14.0\_HF061 (RO55147)
- For a 14.0 policy engine hub on a 64-bit server, apply this hotfix  
integration\_x64\_14.0\_HF062 (RO55147)
- For a 14.0 Remote Policy Engine Connector, apply this hotfix:  
server\_14.0\_HF063 (RO55147)

The list above 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>

## Upgrading iConsole Servers

When you upgrade your iConsole servers, the upgrade procedure installs all the standard searches, upgrading any existing versions, plus upgraded versions of any existing reports. We recommend that you upgrade your iConsole servers in this order:

1. Upgrade your CMS.
2. Upgrade your iConsole application server.
3. Upgrade your iConsole front-end Web servers.
4. (Optional) Rerun the installation wizard to install any additional reports:
  - a. Run setup.exe again on the CMS, your iConsole application server, and each iConsole front-end Web server.
  - b. In the Custom Setup screen of the installation wizard, choose the reports you want to install.

Take care to install the same combination of searches and reports on each server.

5. (Optional) Install BusinessObjects reports for CA DataMinder.

CA DataMinder can integrate with BusinessObjects Enterprise, allowing you to run and customize BusinessObjects reports for CA DataMinder. For deployment details, see the *Reports Integration Guide*.

**Note:** For details about installing iConsole reports, see the 'iConsole Standard Searches, Reports and Policies' chapter in the *Platform Deployment Guide*; search for 'iConsole, reports'.

## Will My Custom Searches Still Run?

The current CA DataMinder release includes essential changes to the iConsole to improve accessibility and usability. Unfortunately, some custom searches and reports may now cause JavaScript errors when a user runs these searches and reports.

As an alternative to fixing your custom searches and reports, we recommend that you review the standard searches and reports that ship with CA DataMinder. You may find that these searches and reports now meet your needs. The standard reports include various reports covering compliance, incidents and issues. It also contains six standard searches. For details, 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 must 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 Orchestra or CA for a specific customer, or one developed by the customer themselves.

## Do I Need To Delete Temporary Internet Files After Upgrading?

If a user needs to use the iConsole within 60 minutes of the iConsole application servers and front-end Web servers being upgraded or a hotfix applied, that user will first need to empty their browser cache to prevent possible Page Errors. For example, to empty the browser cache in Internet Explorer, the user must use the Internet Options dialog to delete all temporary internet files.

This is necessary because JavaScript files required by the iConsole are, by default, cached for one hour on the browser host machine (but see the note below). Consequently, any updated JavaScript files are not available until one hour after the upgrade or hotfix has been applied.

If more than one hour has passed since the upgrade, a user does *not* need to empty their browser cache before using the iConsole. By then, the JavaScript files required by the iConsole will have been automatically updated. For this reason, we recommend that you roll out iConsole upgrades outside of office hours.

**Note:** The cache period, or 'content expiration' time, is configurable in Microsoft IIS on the iConsole front-end Web servers. If this cache period has been lengthened beyond one hour (for example, to reduce network traffic), the period during which iConsole users may experience these Page Errors will also be longer. In this situation, you may want to issue a general advisory to your iConsole users asking them to empty their browser caches.

## Upgrading the Universal Adapter

When you upgrade your Universal Adapter (UA) host servers, the existing Universal Adapter registry values (such as your Input and Output structures) are preserved during the upgrade process.

# Chapter 5: Upgrading from 14.1

---

This section contains the following topics:

[Upgrade CA Business Intelligence 3.2 to 3.3](#) (see page 23)

[Replace Web Triggers with Web-Targeted Data In Motion Triggers](#) (see page 25)

## Upgrade CA Business Intelligence 3.2 to 3.3

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

For the current CA DataMinder release, your reports server must be running BusinessObjects XI 3.1 SP5. In previous releases, CA DataMinder required BusinessObjects XI 3.1 SP4. The simplest way to upgrade from SP4 to SP5 is to install CA Business Intelligence 3.3 on top of your existing CA Business Intelligence 3.2.

**Note:** CA Business Intelligence is a wrapper that includes a BusinessObjects Enterprise installation. You install CA Business Intelligence on your reports server.

### MySQL and Tomcat Are Not Upgraded Automatically

If you do install CA Business Intelligence 3.3 on top of version 3.2, be aware that the upgrade only applies to the BusinessObjects SP level. Existing versions of MySQL and the Tomcat web server are *not* upgraded. After installing CA Business Intelligence 3.3, you must therefore verify that your reports server is running:

- A supported version of Tomcat (6 or later).
- A supported DBMS for the repository database. We do *not* recommend using MySQL in a production environment.

**Note:** Full CA Business Intelligence requirements are in the *Reports Integration Guide*.

### How to Migrate the Repository Database to a New DBMS

(Optional) Follow these guidelines if you want to migrate your existing repository database to a recommended DBMS (for example, from MySQL to SQL Server).

1. Set up the target repository database and a database user account.  
  
For example, if you want to migrate the repository database to SQL Server, create a new BOUSER database login using SQL Server authentication. Then create a new BOREPOS database owned by the BOUSER login.
2. On the reports server, create a new 32-bit system ODBC data source that links to the target repository database as the new database user (BOUSER). You specify this database link as the target database in the migration.
3. Back up BusinessObjects Enterprise for both the source repository database and the <boe> file store locations.

**Note:** 'Copying' data between system database deletes the contents of the source repository database.

4. Follow instructions in the *SAP BusinessObjects Enterprise Administrator's Guide* for copying data between CMS system databases. Find these instructions in the following section:

Managing and Configuring Servers, Configuring Server Settings, Copying Data From One CMS System Database To Another

## Replace Web Triggers with Web-Targeted Data In Motion Triggers

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.

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

Therefore, if you previously used the Internet Explorer agent to control Internet activity, you must perform the following tasks after upgrading to the current version of CA DataMinder.

### **To replace Web triggers with Data In Motion triggers**

Follow these steps:

1. Deploy the network agent on your endpoint computers.

Deployment instructions are in the 'Client Network Agent' chapter of the *Endpoint Integration Guide*.

2. Set up equivalent Data In Motion triggers to replace your old Web triggers.

For example, if you previously used a 'Submitted Text' Web trigger to detect unauthorized data submissions, you can set up a Data In Motion trigger to detect the same data submissions. Remember to set the Which Files Sources? setting to Client Network Agent for File'.

For details about setting up triggers for the network agent, see the 'Stopping Data Leaks to the Cloud' chapter in the *Policy Guide*.



# Chapter 6: Upgrading from 14.0

---

Note the following issues when upgrading from 14.0 to the current CA DataMinder version.

This section contains the following topics:

[Change in 'Data In Use' Behavior for Client File System Agent \(CFSA\)](#) (see page 27)  
[Automatically Reassign Users with Custom Roles to Equivalent 'Official' Roles](#) (see page 28)

[Replace Web Triggers with Web-Targeted Data In Motion Triggers](#) (see page 30)  
[Enable BusinessObjects Reports for CA DataMinder](#) (see page 31)

## Change in 'Data In Use' Behavior for Client File System Agent (CFSA)

The default values for the following machine policy settings changed in release 14.1:

- Client File System Agent/Data in Use Protection/Removable Devices/Default Handling
- Client File System Agent/Data in Use Protection/Network Locations/Default Handling

In pre-14.1 releases, the default values were set to 'Allow Write Access'. They are now set to 'Apply User Policy'.

If you have deployed the File System Agent to your endpoint machines, review these settings in the Common Client Machine Policy and verify that these settings are configured correctly for your requirements.

## Automatically Reassign Users with Custom Roles to Equivalent 'Official' 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.

You can manually reassign these users to existing user roles. Or you can use the 'CustomRoleUpgrade' utility to automate this process.

### About the 'CustomRoleUpgrade' utility

This command line utility creates new user roles that correspond to these various custom roles held by your users. It then reassigns these users to the new user roles. CustomRoleUpgrade saves the new roles and the required user-role assignments in two files:

- A CMS profile file, CRUMachineProfile.xml. This file lists the required new roles. New roles are given default names such as CustomUserRole0013, CustomUserRole0014, and so on. We recommend that you give more meaningful names to these roles. You can rename the roles before implementing the changes on the CMS, or you may find it easier to rename them in the Administration console after implementing the changes.
- An Account Import command file, CRUAccountImport.acc. This file contains the 'setrole' commands that assign users to these new roles.

If you renamed user roles in CRUMachineProfile.xml, you *must* make the corresponding name changes in CRUAccountImport.acc too!

For details about command files for importing users, see the Account Import chapter in the *Platform Deployment Guide*.

To implement these changes, you must manually import these files back onto the CMS.

### To automatically reassign users with custom roles to equivalent official roles

1. Run the following command on the CMS

```
wgninfra -exec wigan/infrastruct/utils/CustomRoleUpgrade CreateFiles
```

This command generates the CMS profile file and Account Import command file. By default, the files are saved in the \System subfolder below the CA DataMinder installation folder.

- (Optional) Rename the new user roles. Edit the CMS profile file and Account Import command file to give more meaningful names to the new roles. Take care to edit the name correctly in both files.

For example, if CustomUserRole0022 is a specialist role for reviewers with responsibility for quarantined events, make the following changes:

**CRUMachineProfile.xml:**

Find the 'role 22' entry:

```
<role index="22">
  <name>CustomUserRole0022</name>
  <privileges>0x43502616420A</privileges>
</role>
```

And change it to this:

```
<role index="22">
  <name>Qarantine Reviewer</name>
  <privileges>0x43502616420A</privileges>
</role>
```

**Important:** Do *not* enclose the role name in double quotes, even if it includes spaces!

**CRUAccountImport.acc**

Find all entries like this:

```
setrole,"unipraxis\oabassi",CustomUserRole0022
```

And change them to this:

```
setrole,"unipraxis\oabassi","Qarantine Reviewer"
```

**Important:** You *must* enclose the role name in double quotes, even if it does not include any spaces!

- Run the following command to import the CMS profile file.  
`wgninfra -exec wigan/infrastructure/machine/Profile Import CRUMachineProfile.xml`  
This command creates the new user roles on the CMS.
- (Optional) If you have not already done so, rename the new user roles. Use the Administration console to give more meaningful names to the new roles:
  - Choose Tools, Manage User Roles.
  - In the Manage User Roles dialog, click the user role that you want to rename.
  - Type the new name for the role.
  - Click OK.
- Run the following Account Import command:  
`wgninfra -exec wigan/infrastructure/accounts/AccountImport Start /in CRUAccountImport.acc`

This command reassigns affected users to the new user roles.

## Replace Web Triggers with Web-Targeted Data In Motion Triggers

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.

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

Therefore, if you previously used the Internet Explorer agent to control Internet activity, you must perform the following tasks after upgrading to the current version of CA DataMinder.

### **To replace Web triggers with Data In Motion triggers**

Follow these steps:

1. Deploy the network agent on your endpoint computers.

Deployment instructions are in the 'Client Network Agent' chapter of the *Endpoint Integration Guide*.

2. Set up equivalent Data In Motion triggers to replace your old Web triggers.

For example, if you previously used a 'Submitted Text' Web trigger to detect unauthorized data submissions, you can set up a Data In Motion trigger to detect the same data submissions. Remember to set the Which Files Sources? setting to Client Network Agent for File'.

For details about setting up triggers for the network agent, see the 'Stopping Data Leaks to the Cloud' chapter in the *Policy Guide*.

## Enable BusinessObjects Reports for CA DataMinder

(Only applies to CA DataMinder customers who want to run BusinessObjects reports for CA DataMinder)

BusinessObjects reports for CA DataMinder are designed to show results by user and group. These reports *do* require event participant data. Before reviewers can run these reports, you must populate the data warehouse with these details. Specifically, you must enable and populate the Event Participant Fact table. There are two methods for populating the Event Participant Fact table:

### Resync the Event Participant Fact table

Use this method if you have never purged events from the CMS database. Events in the CMS already correspond with events in the data warehouse. Specifically, you must:

- a. Manually enable the Event Participant Fact table.
- b. Run a database command to resync the Event Participant Fact table. This operation is relatively fast.

### Truncate and repopulate the data warehouse

Use this method if you regularly purge events from the CMS database.

The data warehouse probably contains data for events that no longer exist in the CMS. You must eliminate this discrepancy before you run BusinessObjects reports. Specifically, you must empty and then repopulate the entire data warehouse so that it only contains events that currently exist in the CMS database. Specifically, you must:

- a. Manually enable the Event Participant Fact table.
- b. Run a database command to truncate and repopulate the data warehouse. This operation takes longer than a resync.
- c. **Note:** If you want to use the iConsole dashboard but not run BusinessObjects reports, you do not need to populate the Event Participant Fact table. The iConsole dashboard has no dependency on the Event Participant Fact table and has no requirement for the table to be enabled.

For details about all of these tasks, see the Data Warehouse chapter of the *Platform Deployment Guide*.



# Chapter 7: Upgrading from 12.5

---

Note the following issues when upgrading from r12.5 to the current CA DataMinder version.

This section contains the following topics:

[Dashboards](#) (see page 33)

[Change in 'Data In Use' Behavior for Client File System Agent \(CFSA\)](#) (see page 36)

[Automatically Reassign Users with Custom Roles to Equivalent 'Official' Roles](#) (see page 37)

[Replace Web Triggers with Web-Targeted Data In Motion Triggers](#) (see page 39)

[Change in AuthenticatedUserType Default Value for ICAP Agent](#) (see page 40)

[Color Coding for Incident Rate By Policy Report](#) (see page 40)

## Dashboards

Previously, the dashboard was based on aggregated data held in database summary tables. Since CA DataMinder 14.0, the iConsole dashboard has been based on data held in the CA DataMinder data warehouse. The data warehouse is a set of database tables containing CA DataMinder event data that has been transformed into a format suitable for generating reports and iConsole dashboards.

Many underlying data warehouse queries run significantly faster than equivalent database queries associated with earlier versions of the Incident Dashboard. Consequently, dashboard performance is significantly faster if you upgrade to the current Incident Dashboard. This improvement is particularly noticeable if your data warehouse includes a very large set of event data.

However, there are some issues associated with upgrades of the dashboard. See the following sections for details.

### **More information:**

[Delay Before the Dashboard is Updated](#) (see page 34)

[Historical Dashboard Data is Lost After Upgrade](#) (see page 35)

## Delay Before the Dashboard is Updated

When you upgrade an iConsole dashboard to the current CA DataMinder version, or when you install a new dashboard, the data warehouse gets populated with your existing events. However, older events may not be included in the dashboard charts and metrics until *the day after the dashboard installation or upgrade*.

If your data warehouse includes over 100,000 events, events more than two months old are not included in the dashboard until the day after the installation or upgrade. This is because the initial data warehousing job for this older data is automatically configured to run during an off-peak window to avoid impacting system performance during office hours. By default, this off-peak window starts at midnight (CMS time) and lasts 300 minutes until 5am, but you can reconfigure it to run when you want.

This delay in displaying older data can also occur if you purge and repopulate the data warehouse. Again, this issue only affects dashboards based on data warehouses with over 100,000 events.

**Note:** Details for rescheduling the initial data warehousing job for older events are described in 'Reschedule the Initial Off-Peak Jobs' in the *Platform Deployment Guide*.

## Historical Dashboard Data is Lost After Upgrade

If you previously maintained long-term incident trend charts in your dashboard, you may lose some (possibly a significant amount) of the underlying historical data when you upgrade CA DataMinder.

Before CA DataMinder 14.0, incident trend charts in the dashboard were generated from database summary tables. Even if the actual events were purged from the CMS database, it was possible to retain aggregated data in these summary tables and thereby maintain long-term incident trend charts in the dashboard.

However, after you upgrade to the current version of CA DataMinder, these summary tables are no longer used. Instead, the incident trends charts are generated from tables in the data warehouse. The data warehouse is populated from the main event tables in the CMS database. Consequently, if you have already purged historical event data from the CMS, these older events cannot be populated into the data warehouse and so cannot be included in the incident trend charts.

### Example

1. Your incident trend charts previously reflected events captured over the period 2008-2012. At the same time, you continually purged events older than 24 months from the CMS database.
2. You upgrade CA DataMinder in 2012. After the upgrade, the CMS only contains events captured since 2010.
3. When the new data warehouse gets populated with event data, it also only contains data for events captured since 2010.
4. Consequently, the new incident trend charts only show data for 2010-2012.

## Change in 'Data In Use' Behavior for Client File System Agent (CFSA)

The default values for the following machine policy settings changed in release 14.1:

- Client File System Agent/Data in Use Protection/Removable Devices/Default Handling
- Client File System Agent/Data in Use Protection/Network Locations/Default Handling

In pre-14.1 releases, the default values were set to 'Allow Write Access'. They are now set to 'Apply User Policy'.

If you have deployed the File System Agent to your endpoint machines, review these settings in the Common Client Machine Policy and verify that these settings are configured correctly for your requirements.

## Automatically Reassign Users with Custom Roles to Equivalent 'Official' 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.

You can manually reassign these users to existing user roles. Or you can use the 'CustomRoleUpgrade' utility to automate this process.

### About the 'CustomRoleUpgrade' utility

This command line utility creates new user roles that correspond to these various custom roles held by your users. It then reassigns these users to the new user roles. CustomRoleUpgrade saves the new roles and the required user-role assignments in two files:

- A CMS profile file, CRUMachineProfile.xml. This file lists the required new roles. New roles are given default names such as CustomUserRole0013, CustomUserRole0014, and so on. We recommend that you give more meaningful names to these roles. You can rename the roles before implementing the changes on the CMS, or you may find it easier to rename them in the Administration console after implementing the changes.
- An Account Import command file, CRUAccountImport.acc. This file contains the 'setrole' commands that assign users to these new roles.

If you renamed user roles in CRUMachineProfile.xml, you *must* make the corresponding name changes in CRUAccountImport.acc too!

For details about command files for importing users, see the Account Import chapter in the *Platform Deployment Guide*.

To implement these changes, you must manually import these files back onto the CMS.

### To automatically reassign users with custom roles to equivalent official roles

1. Run the following command on the CMS

```
wgninfra -exec wigan/infrastruct/utils/CustomRoleUpgrade CreateFiles
```

This command generates the CMS profile file and Account Import command file. By default, the files are saved in the \System subfolder below the CA DataMinder installation folder.

- (Optional) Rename the new user roles. Edit the CMS profile file and Account Import command file to give more meaningful names to the new roles. Take care to edit the name correctly in both files.

For example, if CustomUserRole0022 is a specialist role for reviewers with responsibility for quarantined events, make the following changes:

#### CRUMachineProfile.xml:

Find the 'role 22' entry:

```
<role index="22">  
  <name>CustomUserRole0022</name>  
  <privileges>0x43502616420A</privileges>  
</role>
```

And change it to this:

```
<role index="22">  
  <name>Qarantine Reviewer</name>  
  <privileges>0x43502616420A</privileges>  
</role>
```

**Important:** Do *not* enclose the role name in double quotes, even if it includes spaces!

#### CRUAccountImport.acc

Find all entries like this:

```
setrole,"unipraxis\oabassi",CustomUserRole0022
```

And change them to this:

```
setrole,"unipraxis\oabassi","Qarantine Reviewer"
```

**Important:** You *must* enclose the role name in double quotes, even if it does not include any spaces!

- Run the following command to import the CMS profile file.  

```
wgninfra -exec wigan/infrastructure/machine/Profile Import CRUMachineProfile.xml
```

This command creates the new user roles on the CMS.
- (Optional) If you have not already done so, rename the new user roles. Use the Administration console to give more meaningful names to the new roles:
  - Choose Tools, Manage User Roles.
  - In the Manage User Roles dialog, click the user role that you want to rename.
  - Type the new name for the role.
  - Click OK.
- Run the following Account Import command:  

```
wgninfra -exec wigan/infrastructure/accounts/AccountImport Start /in CRUAccountImport.acc
```

This command reassigns affected users to the new user roles.

## Replace Web Triggers with Web-Targeted Data In Motion Triggers

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.

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

Therefore, if you previously used the Internet Explorer agent to control Internet activity, you must perform the following tasks after upgrading to the current version of CA DataMinder.

### **To replace Web triggers with Data In Motion triggers**

Follow these steps:

1. Deploy the network agent on your endpoint computers.

Deployment instructions are in the 'Client Network Agent' chapter of the *Endpoint Integration Guide*.

2. Set up equivalent Data In Motion triggers to replace your old Web triggers.

For example, if you previously used a 'Submitted Text' Web trigger to detect unauthorized data submissions, you can set up a Data In Motion trigger to detect the same data submissions. Remember to set the Which Files Sources? setting to Client Network Agent for File'.

For details about setting up triggers for the network agent, see the 'Stopping Data Leaks to the Cloud' chapter in the *Policy Guide*.

## Change in AuthenticatedUserType Default Value for ICAP Agent

In the current CA DataMinder release, the AuthenticatedUserType registry value for the ICAP agent defaults to 'auto'. In previous releases, it defaulted to 'DN'.

AuthenticatedUserType specifies what type of user information is included in the ICAP x-header that contains the user credentials. The supported types are distinguished names (DN), 'domain\user' names, and SMTP email addresses. Policy engines use this information to determine which user policy to use when processing the data.

The new 'auto' value enables the ICAP agent to detect the type of user information automatically. Previously, you had to specify which type of user information you wanted the ICAP agent to detect.

When you upgrade to the current CA DataMinder release, you do not need to change the AuthenticatedUserType registry value from 'DN' to 'auto'. However, if you set it to 'auto', the ICAP agent is protected against future changes to your proxy server. For example, if your proxy server switches to ICAP authentication based on SMTP addresses, the ICAP agent cannot identify users while AuthenticatedUserType remains set to 'DN'. Consequently, policy engines apply the Default Policy for Files instead of the policies for the actual users.

## Color Coding for Incident Rate By Policy Report

In the current CA DataMinder release, it is no longer possible to customize the iConsole look-and-feel by editing styles in branded.css to override the base stylesheet.

# Chapter 8: Upgrading Databases

---

This chapter describes the database issues associated with upgrading your CMS.

This section contains the following topics:

[Database Schema Changes](#) (see page 41)

[Pre-upgrade Database Considerations](#) (see page 41)

[Upgrading a Partitioned Oracle Database](#) (see page 42)

[Upgrading the Data Warehouse](#) (see page 51)

[Retrospectively Enable a Data Warehouse After Upgrading](#) (see page 54)

[Performance Enhancements for Searches and Reports](#) (see page 58)

## Database Schema Changes

If you are upgrading your CA DataMinder servers to 14.6, the database schema version is now 3.100. This version includes the following changes.

### **New table Wgn3RelatedEvent (partitioned)**

Contains contains custom Event Grouping details.

**Note:** Full schema details are available in the CA DataMinder *Database Schema and Views Reference Guide*.

## Pre-upgrade Database Considerations

Be aware of the following database issues before starting your upgrade.

### **More information:**

[Back Up Your CMS Database Before Upgrading](#) (see page 41)

[Oracle Issues](#) (see page 42)

## Back Up Your CMS Database Before Upgrading

We strongly recommend that you back up your database, the CA DataMinder registry, and data store before you upgrade your CMS.

## Oracle Issues

Be aware of the following issues:

### Oracle users need extra privilege

Before upgrading your CMS from 12.0, you must manually grant the following privilege to your Oracle primary user and, if specified, the schema owner:

- CREATE MATERIALIZED VIEW

This privilege is granted automatically if upgrading from 14.0 or later.

### CREATE SESSION Privilege

The CREATE SESSION privilege is granted directly to New Search User accounts created for CA DataMinder 14.1 or later. Search User accounts created for earlier versions of CA DLP were granted this privilege indirectly via the CONNECT ROLE.

For a full list of required privileges, see the *Database Guide*; search for 'privileges'.

## Upgrading a Partitioned Oracle Database

You can choose a semi-automated database upgrade method. Or you can fully customize the database upgrade using Native Upgrade scripts provided by CA DataMinder. These methods are described in the following sections.

### More information:

[Semi-automated Database Upgrades](#) (see page 42)

[Native Upgrade Scripts](#) (see page 45)

[Native Script Upgrades from r12.5](#) (see page 47)

[Native Script Upgrades from 14.0](#) (see page 48)

[Native Script Upgrades from 14.1](#) (see page 49)

[Native Script Upgrades from 14.5](#) (see page 50)

## Semi-automated Database Upgrades

(Applies to upgrades from 12.0 or later)

If your database partitioning scheme follows the CA DataMinder default configuration (in terms of naming conventions, the MAXVALUE partition, tablespace, and so on), you can upgrade your Oracle CMS by running the CA DataMinder installation wizard, setup.exe and then manually running a stored procedure after the wizard completes.

If the installation wizard detects a partitioned database, it makes the following changes:

**New partitioned table: Wgn3IssueTrigger**

By default, the installer creates this table in the same tablespace as the Wgn3IssueParticipant table.

This table is named Wgn3IssueTrigger with a single MAXVALUE partition.

After upgrading the CMS, you need to manually run a stored procedure. This automatically adds further partitions to Wgn3IssueTrigger to match the names, size and number of partitions used by other tables in your CMS database.

**New index: Wgn3Trigger.PolicyID**

By default, the installer creates a new index on the PolicyID column in the Wgn3Trigger table. In a partitioned database, it creates a local index in the same tablespace as the index on Wgn3Trigger.TriggerName.

**New partitioned table: Wgn3RelatedEvent**

By default, the installer creates this table in the Default tablespace unless the customization specifies a different location.

This table is named Wgn3RelatedEvent with a single MAXVALUE partition.

After upgrading the CMS, you need to manually run a stored procedure (Wgn\_Partition\_Util.wgn\_partition\_new\_table()). This automatically adds further partitions to Wgn3RelatedEvent to match the names, size, and number of partitions used by other tables in your CMS database.

**To perform a semi-automated upgrade**

1. Run setup.exe on the server hosting the CMS.

Find this file in the root of the CA DataMinder distribution image.

CA DataMinder automatically detects that you are upgrading and launches the server installation wizard.

2. Follow the on-screen instructions. Continue to the final wizard screen and click Install.
3. Run a stored procedure to modify the newly-created database table, Wgn3IssueTrigger, so that it matches the other partitioned tables in your database in terms of size, number and names of partitions.

This stored procedure was installed when you upgraded your CMS. It is called: WGN\_PARTITION\_UTIL.WGN\_PARTITION\_12\_5\_TABLES

4. Run the following command to modify the newly-created database table Wgn3RelatedEvent, so that it matches the other partitioned tables in your database in terms of size, number, and names of partitions.

```
SQL> EXEC Wgn_Partition_Util.wgn_partition_new_table(  
    new_table_name => 'WGN3RELAETEDEVENT',  
    template_name  => 'WGN3EVENT',  
    pdebug         => True,  
    db_type        => Wgn_Partition_Util.wgn_db_type_CMS,  
    Tablespace_Name =>  
    Wgn_Partition_Util.wgn_get_tablespace_name('WGN3RELAETEDEVENT')  
);
```

## Native Upgrade Scripts

CA DataMinder provides Native Upgrade scripts for customers who require flexibility in managing the database for their Oracle CMS. For example, these scripts enable DBAs to use their own tablespace and partition naming conventions.

**Important!** Always use a version of SQL\*Plus that matches your version of Oracle. Errors can occur if you use an older version of SQL\*Plus to run scripts against a newer version of Oracle.

Find the Native Upgrade scripts in the CA DataMinder distribution image. Browse to the \Support\NativeSchemaSQL\ORACLE\Partitioned folder. This folder contains the following subfolders:

### \Install

The scripts in this folder are for customers installing a new partitioned CMS. They are not needed when upgrading an existing Oracle CMS.

### \UpgradeV12\_0ToV12\_5

You need the scripts in this folder if you are upgrading a partitioned r12.0 CMS where the database is partitioned and/or you need to customize physical attributes of objects in the upgrade.

**Note:** After upgrading from 12.0, you must run a table partitioning stored procedure.

### \UpgradeV12\_5ToV14\_0

You need the scripts in this folder if you are upgrading a partitioned r12.5 CMS where the database is partitioned and/or you need to customize physical attributes of objects in the upgrade.

If you are upgrading from 12.0, these scripts comprise the second stage in the pre-upgrade process.

### \UpgradeV14\_0ToV14\_1

You need the scripts in this folder if you are upgrading a partitioned 14.0 CMS where the database is partitioned and/or you need to customize physical attributes of objects in the upgrade.

If you are upgrading from:

- 12.0, these scripts comprise the third stage in the pre-upgrade process.
- 12.5, these scripts comprise the second stage in the pre-upgrade process.

#### **\UpgradeV14\_1ToV14\_5**

You need the scripts in this folder if you are upgrading a partitioned 14.1 CMS where the database is partitioned and/or you need to customize physical attributes of objects in the upgrade.

If you are upgrading from:

- 12.0, these scripts comprise the fourth stage in the pre-upgrade process.
- 12.5, these scripts comprise the third stage in the pre-upgrade process.
- 14.0, these scripts comprise the second stage in the pre-upgrade process.

#### **\UpgradeV14\_5ToV14\_6**

You need the scripts in this folder if you are upgrading a partitioned 14.5 CMS where the database is partitioned and/or you need to customize physical attributes of objects in the upgrade.

If you are upgrading from:

- 12.5, these scripts comprise the fourth stage in the pre-upgrade process.
- 14.0, these scripts comprise the third stage in the pre-upgrade process.
- 14.1, these scripts comprise the second stage in the pre-upgrade process.

## Native Script Upgrades from r12.5

These instructions upgrade your CA DataMinder database from 12.5 to 14.0.

### To upgrade from r12.5 using the native upgrade scripts

1. Go to the \UpgradeV12\_5ToV14 subfolder in your CA DataMinder distribution image.

2. Copy this subfolder to your database host server.

This subfolder includes Native\_UpgradeToVer3\_70.sql and Native\_Wrapper.sql.

3. Edit Native\_UpgradeToVer3\_70.sql on your database host server to make the changes you require.

4. Run the following command as the schema owner, using the SQL\*Plus utility:

```
SQL> set serveroutput on size unlimited
SQL> start Native_Wrapper.sql;
```

**Important!** Always use a version of SQL\*Plus that matches your version of Oracle. Errors can occur if you use an older version of SQL\*Plus to run scripts against a newer version of Oracle.

5. (Optional) Install the Data Warehouse. Run the CA DataMinder server installation wizard or, if you want to customize storage for the data warehouse, run the data warehouse native scripts.

- **Native DDL scripts:** For instructions, see the 'Database Storage and Partitioning' chapter in the *Database Guide*.
- **Server installation wizard:** For instructions, see the 'Data Warehouse' chapter in the *Platform Deployment Guide*.

6. Upgrade the CMS by running setup.exe.

Find setup.exe in the root of your CA DataMinder distribution image. For details about installing a CMS, see the *Platform Deployment Guide*.

7. (Optional) Run the following command to create a partitioned Data Warehouse with partition dates that match the CMS.

Run this command as the schema owner, using the SQL\*Plus utility:

```
SQL> EXEC Wgn_Partition_Util.wgn_partition_tables(
  partition_dates =>
  Wgn_Partition_Util.get_partition_dates(Wgn_Partition_Util.wgn_db_type_cms)
  , db_type => Wgn_Partition_Util.wgn_db_type_DW
  , Partition_Options => Wgn_Partition_Util.wgn_opt_Convert_to_Partitioned
  , new_tablespace => 'WGNDATADW'
  , new_indextablespace => 'WGNDATADWIDX'
  , pdebug => True );
```

8. You now need to upgrade from 14.0. See the next section.

## Native Script Upgrades from 14.0

These instructions upgrade your CA DataMinder database from 14.0 to 14.1.

### To upgrade from 14.0 using the native upgrade scripts

1. Go to the \UpgradeV14\_0ToV14\_1 subfolder in your CA DataMinder distribution image.

2. Copy this subfolder to your database host server.

This subfolder includes Native\_UpgradeToVer3\_80.sql and Native\_Wrapper.sql.

3. Edit Native\_UpgradeToVer3\_80.sql on your database host server to make the changes you require.

4. Run the following command as the schema owner, using the SQL\*Plus utility:

```
SQL> set serveroutput on size unlimited
SQL> start Native_Wrapper.sql;
```

**Important!** Always use a version of SQL\*Plus that matches your version of Oracle. Errors can occur if you use an older version of SQL\*Plus to run scripts against a newer version of Oracle.

5. Upgrade the data warehouse. Do one of the following:

- Run the CA DataMinder server installation wizard. For instructions, see the 'Data Warehouse' chapter in the *Platform Deployment Guide*.
- Run the data warehouse native DDL scripts if you want to customize storage for the data warehouse. For instructions, see the 'Database Storage and Partitioning' chapter in the *Database Guide*.

6. Upgrade the CMS by running setup.exe.

Find setup.exe in the root of your CA DataMinder distribution image. For details about installing a CMS, see the *Platform Deployment Guide*.

7. (Optional) Follow this step only if you have a pre-existing 14.0 data warehouse that is *not* currently partitioned.

The following command partitions your data warehouse with partition dates that match the CMS. Run this command as the schema owner, using the SQL\*Plus utility:

```
SQL> EXEC Wgn_Partition_Util.wgn_partition_tables(
    partition_dates =>
Wgn_Partition_Util.get_partition_dates(Wgn_Partition_Util.wgn_db_type_cms)
    , db_type => Wgn_Partition_Util.wgn_db_type_DW
    , Partition_Options => Wgn_Partition_Util.wgn_opt_Convert_to_Partitioned
    , new_tablespace => 'WGNDATADW'
    , new_indextablespace => 'WGNDATADWIDX'
    , pdebug => True );
```

8. You now need to upgrade from 14.1. See the next section.

## Native Script Upgrades from 14.1

These instructions upgrade your CA DataMinder database from 14.1 to 14.5.

### To upgrade from 14.1 using the native upgrade scripts

1. Go to the \UpgradeV14\_1ToV14\_5 subfolder in your CA DataMinder distribution image.
2. Copy this subfolder to your database host server.

This subfolder includes Native\_UpgradeToVer3\_90.sql and Native\_Wrapper.sql.

3. Run the following command as the schema owner, using the SQL\*Plus utility:

```
SQL> set serveroutput on size unlimited
SQL> start Native_Wrapper.sql;
```

**Important!** Always use a version of SQL\*Plus that matches your version of Oracle. Errors can occur if you use an older version of SQL\*Plus to run scripts against a newer version of Oracle.

4. Upgrade the data warehouse.

Run the CA DataMinder server installation wizard. For instructions, see the 'Data Warehouse' chapter in the *Platform Deployment Guide*.

5. Upgrade the CMS by running setup.exe.

Find setup.exe in the root of your CA DataMinder distribution image. For details about installing a CMS, see the *Platform Deployment Guide*.

## Native Script Upgrades from 14.5

These instructions upgrade your CA DataMinder database from 14.5 to 14.6.

### To upgrade from 14.5 using the native upgrade scripts

1. Go to the \UpgradeV14\_5ToV14\_6 subfolder in your CA DataMinder distribution image.
2. Copy this subfolder to your database host server.

This subfolder includes Native\_UpgradeToVer3\_100.sql and Native\_Wrapper.sql.

3. Run the following command as the schema owner, using the SQL\*Plus utility:

```
SQL> set serveroutput on size unlimited
SQL> start Native_Wrapper.sql;
```

**Important!** Always use a version of SQL\*Plus that matches your version of Oracle. Errors can occur if you use an older version of SQL\*Plus to run scripts against a newer version of Oracle.

4. Upgrade the data warehouse.

Run the CA DataMinder server installation wizard. For instructions, see the 'Data Warehouse' chapter in the *Platform Deployment Guide*.

5. Upgrade the CMS by running setup.exe.

Find setup.exe in the root of your CA DataMinder distribution image. For details about installing a CMS, see the *Platform Deployment Guide*.

Run this command as the schema owner, using the SQL\*Plus utility:

```
SQL> EXEC Wgn_Partition_Util.wgn_partition_new_table(
      new_table_name => 'WGN3RELADEEVENT',
      template_name  => 'WGN3EVENT',
      pdebug         => True,
      db_type        => Wgn_Partition_Util.wgn_db_type_CMS,
      Tablespace_Name =>
Wgn_Partition_Util.wgn_get_tablespace_name('WGN3RELADEEVENT')
);
```

This command partitions the new WGN3RELADEEVENT table with partition dates that match the Wgn3Event.

## Upgrading the Data Warehouse

When you upgrade your CA DataMinder data warehouse, you can choose a fully automated upgrade, or you can customize the upgrade using Native Upgrade scripts provided by CA DataMinder.

### Fully Automated Upgrade

You upgrade your data warehouse at the same time as you upgrade your CMS.

1. Run setup.exe on the server hosting the CMS and data warehouse.  
Find this file in the root of the CA DataMinder distribution image.  
CA DataMinder automatically detects that you are upgrading and launches the server installation wizard.
2. Follow the on-screen instructions. Continue to the final wizard screen and click Install.

### Native Script Upgrade

(Oracle data warehouses only) If you prefer to upgrade your data warehouse by running native scripts, follow these steps:

1. Run a native script to upgrade the data warehouse tables.
2. Upgrade the data warehouse:
  - a. Run setup.exe on the server hosting the CMS and data warehouse.  
Find this file in the root of the CA DataMinder distribution image.  
CA DataMinder automatically detects that you are upgrading and launches the server installation wizard.
  - b. Follow the on-screen instructions. Continue to the final wizard screen and click Install.
3. (Optional) Partition the new data warehouse tables that were added in the current CA DataMinder release.

Steps 1 and 3 are described in the following sections.

### More information:

[Run a Native Script to Upgrade the Data Warehouse](#) (see page 52)  
[Partition the New Data Warehouse Tables](#) (see page 54)

## Run a Native Script to Upgrade the Data Warehouse

(Oracle data warehouses only)

This procedure upgrades the data warehouse tables. There is a separate procedure for upgrading the main CMS database tables using native scripts.

**Note:** You do not need to create a separate database schema owner and primary user account. The data warehouse uses the same accounts that you created when running the native script for the main CMS database tables, `native_wrapper.sql`.

### Upgrade the data warehouse tables

1. Verify that you have modified the `DWGrant_user.sql` script to reference the primary user.

(Optional) Verify that you have modified the `DWSynonyms.sql` script to reference the schema owner.

For details, see [Modify the Grant\\_User and Synonyms Scripts](#).

2. Copy the modified script files to a location where SQL\*Plus can access them.

3. Browse to the folder containing the script files and open Native\_DWWrapper.sql.
4. Start SQL\*Plus, and connect to the database as the user who will own the CA DataMinder schema tables. That is, you must connect as the:
  - **Schema owner** if you **have** created a separate schema owner, or  
**Primary user** if you have **not** created a separate schema owner.
5. From the SQL\*Plus prompt, type:

```
start native_dwrapper
```

This upgrades the tables and indexes, and populates the tables with basic data.
6. Review the native-dwrapper.log file to confirm that the script executed correctly.
7. If you **have** created separate Primary User and Schema Owner accounts, go to step 8.

If you do not have separate accounts (that is, the primary user also owns the CA DataMinder schema tables), this completes the script installation.
8. You now need to grant the primary user access to the tables you created in step 5, and create synonyms for this user.
  - a. Verify that you are connected to the database as the schema owner.
  - b. In SQL\*Plus, type this command:

```
start DWGrant_user
```
  - c. Still in SQL\*Plus, reconnect to the database as the primary user. See step 4 for command details.
  - d. To create the Oracle synonyms against the primary user, type this command:

```
start dwsynonyms
```

This completes the native script upgrade for the data warehouse.
9. If you have not yet upgraded the CMS, run setup.exe to upgrade the CMS and the date warehouse together.

If you have already upgraded the CMS, run setup.exe to upgrade the date warehouse only.

## Partition the New Data Warehouse Tables

(Optional)

New data warehouse tables have been added in the current version of CA DataMinder. If your data warehouse was partitioned in a previous version of CA DataMinder, you must execute a procedure in the Wgn\_Partition\_Util core package to partition the new tables.

The following command partitions the new tables in your data warehouse. Use SQL\*Plus to run this command as the schema owner:

```
SQL> EXEC Wgn_Partition_Util.wgn_partition_tables
(
  partition_dates => WGN_PARTITION_DATES_TAB(),
  db_type => Wgn_Partition_Util.wgn_db_type_DW,
  Partition_Options => Wgn_Partition_Util.wgn_opt_Partition_NonPart_Tabs,
  pdebug => True
);
```

**Note:** For details about the Wgn\_Partition\_Util core package, see the Database Storage and Partitioning chapter in the *Database Guide*.

## Retrospectively Enable a Data Warehouse After Upgrading

If you did not enable the data warehouse in a previous version of CA DataMinder, the data warehouse remains disabled when you upgrade to the current version of CA DataMinder. However, you can manually enable the data warehouse.

### How To Manually Enable the Data Warehouse After Upgrading CA DataMinder

1. (Optional) Set credentials for the Reporting User database account.  
You only need this database account if you intend to run BusinessObjects reports.
2. (Optional) Set credentials for the Unrestricted Search User database account.  
You only need this database account if you intend to run BusinessObjects reports.
3. Enable the Data Warehouse in the Administration console.
4. (Optional) Configure the Data Warehouse to support BusinessObjects reports.

**Note:** For full details about managing the data warehouse, including advanced configuration for data warehousing jobs, see the 'Data Warehouse' chapter in the *Platform Deployment Guide*.

**More information:**

[Set Credentials for the Reporting User](#) (see page 55)

[Set Credentials for the Unrestricted Search User](#) (see page 56)

[Enable the Data Warehouse After Installing](#) (see page 57)

[Configure Support for BusinessObjects Reports](#) (see page 58)

## Set Credentials for the Reporting User

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

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

### To set credentials for the Reporting User

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

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

```
CREATE SESSION  
RESOURCE  
DBA  
SYSDBA
```

### **When must I provide Database Administrator details?**

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

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

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

## **Set Credentials for the Unrestricted Search User**

Before you enable the Data Warehouse, you may need to specify the Unrestricted Search User database account.

This database account corresponds to the 'Unrestricted' security model. CA DataMinder consoles and external reporting tools can use this database account when searching the CA DataMinder Data Warehouse and CMS database for events. Unlike normal Search User database accounts, the Unrestricted Search User is *not* subject to row level security (RLS) when searching the database. If a reviewer has 'Unrestricted' security model, the reviewer can see any events when they run a search or report. Search results or reports are not restricted by policy class or the reviewer's management group.

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

### **To set credentials for the Unrestricted Search User**

1. Log on to the Administration console using an account that has the 'Admin: Manage security models' privilege.
2. Click Tools, Manage Security Models.
3. In the Manage Security Models dialog, select the Unrestricted model and click Modify.

4. In the Modify Security Model dialog, click Set Credentials.
5. In the Set Model Credentials dialog, enter the user name and password.
6. (Optional) If necessary, provide credentials for an existing Database Administrator account. See below for details.

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

```
CREATE SESSION
RESOURCE
DBA
SYSDBA
```

#### **When must I provide Database Administrator details?**

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

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

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

## **Enable the Data Warehouse After Installing**

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

#### **To enable the Data Warehouse**

1. Log on to the Administration console using an account that has the 'Admin: Manage security models' privilege.
2. Click Tools, Configure Data Warehouse.
3. In the General Options section, select the 'Enable Data Warehouse population' check box.
4. (Optional) Configure other Data Warehouse settings as required.

## Configure Support for BusinessObjects Reports

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

BusinessObjects reports for CA DataMinder show results by user and group. These reports therefore require event participant data. Before reviewers can run these reports, you must populate the Data Warehouse with this data.

### To configure the Data Warehouse to support BusinessObjects reports

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

The Configure Data Warehouse dialog displays.

3. In the General Options section, select the 'Collect event participant data' check box.
4. (Applies only if you already use the iConsole dashboard). Resynchronize, or empty and repopulate, the Data Warehouse.

If you already use the iConsole dashboard, your Data Warehouse already contains event and audit data. However, it does not contain event participant data. You must now add this data to the Data Warehouse. Do *one* of the following:

- Go to the Advanced Options section and select the 'Resynchronize Data Warehouse data on next run' check box.

Use this method if you have never purged events from the CMS database. Events in the CMS already correspond with events in the data warehouse. This operation is relatively fast.

- Go to the Advanced Options section and select the 'Purge all Data Warehouse data and repopulate on next run' check box.

Use this method if you regularly purge events from the CMS database. The Data Warehouse probably contains data for events that no longer exist in the CMS. You must eliminate this discrepancy before you run BusinessObjects reports. Specifically, you must empty and then repopulate the entire Data Warehouse so that it only contains events that currently exist in the CMS database. This operation takes longer than a resync.

## Performance Enhancements for Searches and Reports

(Optional) You can the following post-upgrade stored procedures on the CMS to optimize CA DataMinder search and report performance.

**More information:**

[Stored procedure: wgn\\_queryflags\\_migrate](#) (see page 59)

## Stored procedure: `wgn_queryflags_migrate`

(Optional) You can run a post-upgrade stored procedure (`Wgn_Queryflags_Migrate`) on the CMS to optimize CA DataMinder search and report performance.

This stored procedure (SP) migrates key data to a new database column and can take a long time. The CMS runs as normal while data is being migrated. However, we recommend that you schedule the SP to run during off-peak periods, typically outside of office hours.

After the SP has completed, we strongly recommend that you defragment your database indexes (see below).

**Note:** During testing, we observed migration rates of up to 6 million events per hour. However, actual migration rates in a production environment depend on your hardware configuration and data distribution.

### Run the Wgn\_Queryflags\_Migrate SP

The procedure differs, depending on your database engine.

#### Oracle CMSs

In Oracle SQL\*Plus, connect to the CA DataMinder database as the schema owner. If there is no separate account for the schema owner, connect as the primary user.

**Important!** If your Oracle database has separate accounts for the primary user and the schema owner, you *must* run the Wgn\_Queryflags\_Migrate SP as the schema owner (for example, WGNOWNER). Do not run this SP as the primary user (for example, WGNUSER). This is because the SP is created under the schema owner and there are no grants or synonyms. If you do not have separate accounts for the primary user and the schema owner, run the SP as the primary user.

Run the following commands:

```
SQL> set serveroutput on size unlimited
SQL> EXEC wgn_queryflags_migrate;
```

#### SQL Server CMSs

Log in to SQL Server Management Studio as the primary user. Then run the following command:

```
EXECUTE dbo.wgn_queryflags_migrate
```

#### Prototype

The SP prototype is shown below:

```
Wgn_Queryflags_Migrate (
    BatchSize IN NUMBER,
    UpdateBatchSize IN NUMBER
    TimeOutMins IN NUMBER
    RestartMigrate IN NUMBER
);
```

Where:

#### Batchsize

Defaults to 10,000. Specifies the number of events migrated in each batch.

#### UpdateBatchsize

(SQL Server only) Defaults to 10,000. Specifies the maximum number of rows updated in each batch.

#### TimeOutMins

Defaults to zero. Specifies the period (in minutes) before the SP times out. Use this parameter to restrict how long the SP runs. For example, if you schedule the SP to start at midnight, set this parameter to 180 (four hours) to stop the SP at 3am.

When you restart the SP after a timeout, the SP resumes migrating events at the point where it stopped.

If this parameter is set to zero, the SP never times out.

#### **RestartMigrate**

Defaults to zero. Restarts the SP process.

**Oracle Example:** This example sets the batch size to 50,000 with a three hour timeout. You must run a preliminary command before executing the SP:

```
SQL> set serveroutput on size unlimited  
SQL> EXEC Wgn_QueryFlags_Migrate (Batchsize => 50000, TimeOutMins => 180);
```

**SQL Server Example:** This example sets the batch size to 50,000 with a three hour timeout and limits the number of updated rows in each batch to 10,000:

```
EXECUTE dbo.Wgn_QueryFlags_Migrate @Batchsize = 50000, @UpdateBatchsize = 10000,  
@TimeOutMins = 180
```

#### **Defragment the Database Indexes**

After the SP has completed, some database indexes will be heavily fragmented because of the data updates. We strongly recommend that you run your standard index maintenance routines at the earliest convenient opportunity to remove any temporary performance degradation due to this index fragmentation.



# Index

---

## A

ASP.NET, for iConsole • 15

## B

before upgrading • 13

## C

CMS • 14

    back up and suspend • 14

Custom base policies • 12

## D

database • 41

    upgrade issues • 41

## I

iConsole • 15

    .NET Framework • 15

## K

known issues when upgrading • 41

    databases • 41

## M

major and minor changes to policy schema • 11

## N

.NET Framework, for iConsole • 15

## P

policy transfers • 11

pre-upgrade tasks • 13

## U

Universal Adapter • 22