This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2012 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.

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: Upgrading CA DLP**

- About This Guide ................................................................................................................. 9
- Version, Policy and File Compatibility .........................................................................................10
  - CMS ..................................................................................................................................... 11
  - Client Machines .....................................................................................................................11
  - iConsole Servers ...................................................................................................................12
  - Event Files and Search Files .................................................................................................12
  - Policy Transfers ....................................................................................................................13
  - Custom Base Policies ............................................................................................................14
- Features No Longer Supported ................................................................................................15

**Chapter 2: Pre-Upgrade Tasks**

- Migrate Registry Values .............................................................................................................20
- Back Up and Suspend the CMS ..................................................................................................21
- Upgrade .NET Framework on iConsole Servers .........................................................................21

**Chapter 3: Upgrade Procedures**

- Recommended Upgrade Sequence .............................................................................................23
- How to Upgrade a CA DLP Computer ......................................................................................24
- Upgrading the CMS ....................................................................................................................25
- Upgrading iConsole Servers ....................................................................................................26
  - Will My Custom Searches Still Run? .....................................................................................26
  - Do I Need To Delete Temporary Internet Files After Upgrading? ........................................27
- Upgrading the Universal Adapter ...............................................................................................28

**Chapter 4: Upgrading from 6.0**

- Upgrading a 6.0 Database ..........................................................................................................29
- Reboot Your CA DLP Servers ....................................................................................................30
- Default Policy for Imported or Scanned Files ..........................................................................30
- Upgrading the iConsole ..............................................................................................................30
  - Manually Upgrade Standard Searches, Reports and Dashboards ........................................31
  - Respecify Customized Reports Based on Policy or Class .....................................................31
  - Color Coding for Incident Rate By Policy Report ..................................................................32
  - Update Virtual Directory References in iConsole Bookmarks ............................................32
  - Drop-Down Recipient Lists in Compose Mail Dialog ...........................................................33
Chapter 5: Upgrading from 12.0

Reboot Your CA DLP Servers ............................................................................................................. 39
Security Models ..................................................................................................................................... 40
Upgrading the iConsole .......................................................................................................................... 40
   Color Coding for Incident Rate By Policy Report .............................................................................. 40
   New Location For Custom iConsole Images .................................................................................... 41
Dashboards ............................................................................................................................................ 41
   Delay Before the Dashboard is Updated ............................................................................................ 42
   Historical Dashboard Data is Lost After Upgrade ............................................................................... 43
Administrative Privilege Renamed ........................................................................................................ 43
Log Files Are Not Relocated .................................................................................................................. 44
FSA Remote Connector Upgrades on 64-bit Machines ...................................................................... 45
Change in AuthenticatedUserType Default Value for ICAP Agent ..................................................... 46

Chapter 6: Upgrading from 12.5

Dashboards ............................................................................................................................................ 47
   Delay Before the Dashboard is Updated ............................................................................................ 48
   Historical Dashboard Data is Lost After Upgrade ............................................................................... 49
Color Coding for Incident Rate By Policy Report .............................................................................. 49
Change in AuthenticatedUserType Default Value for ICAP Agent ..................................................... 50

Chapter 7: Upgrading Databases

Database Schema Changes ..................................................................................................................... 52
Pre-upgrade Database Considerations .................................................................................................. 52
   Back Up Your CMS Database Before Upgrading ............................................................................ 53
   Oracle Issues .................................................................................................................................... 53
Database Schema Change ...................................................................................................................... 54
Upgrading a Partitioned Oracle Database ............................................................................................. 54
   Semi-automated Database Upgrades ................................................................................................. 55
   Native Upgrade Scripts ..................................................................................................................... 56
   Native Script Upgrades from 6.0 ....................................................................................................... 57
   Native Script Upgrades from r12.0 .................................................................................................... 59
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading from r12.5</td>
<td>62</td>
</tr>
<tr>
<td>Upgrading a 6.0 Database</td>
<td>63</td>
</tr>
<tr>
<td>What Database Changes Are Needed?</td>
<td>63</td>
</tr>
<tr>
<td>How to Upgrade a 6.0 Database</td>
<td>64</td>
</tr>
<tr>
<td>Oracle: Post-Upgrade Change To Event Participant Table</td>
<td>67</td>
</tr>
<tr>
<td>SQL Server: Post-Upgrade Change To Event Participant Table</td>
<td>68</td>
</tr>
<tr>
<td>Enabling the Data Warehouse</td>
<td>78</td>
</tr>
<tr>
<td>Specify the Data Warehouse User</td>
<td>79</td>
</tr>
<tr>
<td>Specify the Unrestricted Search User</td>
<td>80</td>
</tr>
<tr>
<td>Manually Enable the Data Warehouse</td>
<td>81</td>
</tr>
<tr>
<td>Enable the Event Participant Fact Table</td>
<td>81</td>
</tr>
<tr>
<td>Appendix A: Accessibility Features</td>
<td>83</td>
</tr>
<tr>
<td>Display</td>
<td>83</td>
</tr>
<tr>
<td>Sound</td>
<td>84</td>
</tr>
<tr>
<td>Keyboard</td>
<td>84</td>
</tr>
<tr>
<td>Mouse</td>
<td>85</td>
</tr>
<tr>
<td>Index</td>
<td>87</td>
</tr>
</tbody>
</table>
Chapter 1: Upgrading CA DLP

This guide describes how to upgrade 6.0, 12.0, and 12.5 deployments to CA DLP 14.0. 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 version 4.x or 5.0 (when the product was called 'Orchestria APM'). If you want to upgrade from these versions, contact Technical Support.

This section contains the following topics:

About This Guide (see page 10)
Version, Policy and File Compatibility (see page 11)
Features No Longer Supported (see page 15)
About This Guide

This guide contains the following chapters:

Upgrading CA DLP

This chapter contains the following sections:

Version and Policy Compatibility

This section describes how CA DLP handles data transfers (policy changes and captured data) between machines running different versions of the product.

Features No Longer Supported

This section describes any features or components no longer supported in the current CA DLP version.

Pre-upgrade Tasks

This chapter specifies which areas of the CA DLP enterprise may need checking before starting an upgrade.

Important! If upgrading from version 6.0, you must migrate the old Orchestria registry keys before you upgrade! You must do this on every CA DLP machine!

Upgrade Procedure

This chapter describes the order in which we recommend you upgrade your CA DLP machines.

It also describes any specific upgrade tasks needed for machines hosting individual CA DLP components.

Post-upgrade Issues

This chapter identifies the post-upgrade issues when upgrading from versions 6.0, 12.0 and 12.5 respectively.

Database Upgrade Issues

This chapter describes specific upgrade tasks for your CA DLP database.

This is particularly important if upgrading from version 6.0 due to schema changes and security model changes introduced in version 12.0.

More information:

Pre-Upgrade Tasks (see page 19)
Version, Policy and File Compatibility (see page 11)
Upgrade Procedures (see page 23)
Version, Policy and File Compatibility

Upgrading individual CA DLP machines is simple. In principle, we recommend that you upgrade all your CA DLP 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 DLP handles data transfers (policy changes and captured data) between machines running different versions of the product.

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

**CMS**

There are no known issues connecting an upgraded CMS to earlier version CA DLP components, with the exception of the iConsole.

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 DLP, the iConsole may not function correctly.

For example, we do not support 14.0 iConsole servers connected to a 12.5 CMS. Likewise, we do not support 12.5 iConsole servers connected to a 14.0 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 DLP supports EVF, EVL, EVS and QDF files generated by all earlier versions of CA DLP.
Policy Transfers

Following a CA DLP upgrade, policy compatibility between servers and client machines running different versions of CA DLP 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 DLP 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 DLP 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 DLP upgrade.
   c. You then need to apply the updated base policies.

Note: We strongly recommend you apply for updated base policies before upgrading.
Features No Longer Supported

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

CA DLP version 5.0

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

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

Symantec Enterprise Vault 6.0 SP3

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

EMC SourceOne Email Management 6.5 SP1

CA DLP 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 DLP supports SourceOne 6.6 SP1.
Features No Longer Supported

Personal Audit Report (PAR)

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

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 DLP 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 DLP continues to support:

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

- Actiance (formerly 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 DLP 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 DLP, 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 2: 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 20)
- **Back Up and Suspend the CMS** (see page 21)
- **Upgrade .NET Framework on iConsole Servers** (see page 21)
Migrate Registry Values

(Only required if upgrading from version 6.00)

Important! If upgrading from version 6.0, you must migrate the old Orchestria registry keys on every CA DLP machine before you upgrade!

In r12.0, the registry key used by CA DLP components changed:

- In 6.0, the product registry key was:
  HKEY_LOCAL_MACHINE\SOFTWARE\Orchestria\Active Policy Management
- In r12.0 and later, the product registry key is:
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA DLP

New product installations automatically use the new CA DLP registry key, but upgrades from 6.0 require a manual registry fix. Specifically, before you upgrade any CA DLP server (including the CMS), or any client machine or utility machine, you must run the migreg.exe utility to copy existing registry values to the new key. The upgrade is blocked if the installation wizard detects that registry values have not been migrated to the new key.

1. Find migreg.exe in the\Support folder on your CA DLP distribution media. We recommend that you copy this utility to a suitable network location.

2. Before you upgrade a CA DLP machine, run this command locally:
   
   `<path>\migreg -m`
   
   Where `<path>` specifies the migreg.exe location you chose in step 1.

3. After successfully upgrading all CA DLP components on a machine, you can optionally run this command to purge the old Orchestria 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 DLP installation folder on the CMS:

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

**Upgrade .NET Framework on iConsole Servers**

For the current version of CA DLP, 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 3: Upgrade Procedures

This section contains the following topics:

- **Recommended Upgrade Sequence** (see page 23)
- **How to Upgrade a CA DLP Computer** (see page 24)
- **Upgrading the CMS** (see page 25)
- **Upgrading iConsole Servers** (see page 26)
- **Upgrading the Universal Adapter** (see page 28)

**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 DLP

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 DLP 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 DLP 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 DLP Computer**

All CA DLP upgrades can now be run using a single executable, setup.exe. CA DLP automatically detects that you are upgrading and launches the appropriate installation wizard.

**To upgrade your CA DLP enterprise**

1. Run setup.exe on the various host computers.
   - Find this file in the root of the CA DLP distribution image.

2. This launches the CA DLP server installation wizard.
   - 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.

**Licenses**

When the CMS upgrade is complete, you may need to reinstall your license files, or install new license files before you can start using CA DLP.

Your license files unlock the policy modules available to your organization. For information about obtaining and installing license files, see the Administration console online help—search for 'license files'.

**More information:**

[Oracle Issues](#) (see page 53)
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 DLP.
   CA DLP can integrate with [assign the value for boe in your book], allowing you to run and customize BusinessObjects reports for CA DLP. 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 DLP 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 DLP. 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 Orchestria 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 4: Upgrading from 6.0

Note the following issues when upgrading from version 6.0 (when the product was known as Orchestria APM) to the current CA DLP version.

This section contains the following topics:
- **Upgrading a 6.0 Database** (see page 29)
- **Reboot Your CA DLP Servers** (see page 30)
- **Default Policy for Imported or Scanned Files** (see page 30)
- **Upgrading the iConsole** (see page 30)
- **Dashboards** (see page 34)
- **Upgrading FSA Jobs** (see page 36)
- **Review Queue** (see page 37)
- **Log Files Are Not Relocated** (see page 37)

**Upgrading a 6.0 Database**

In r12.0, schema changes were made to the Wgn3EventParticipant database table to accommodate changes to security model handling. At the same time, any participant records in this table associated with Web and Application Monitor events must be updated.

Consequently, the database upgrade process from 6.0 requires a pre- and post-upgrade steps. These steps are described in the 'Upgrading Databases' chapter. See the reference below for details.

More information:
- **Upgrading a 6.0 Database** (see page 63)
- **What Database Changes Are Needed?** (see page 63)
- **How to Upgrade a 6.0 Database** (see page 64)
Reboot Your CA DLP Servers

Changes to the infrastructure in the current version of CA DLP mean that any servers running the CA DLP infrastructure must be rebooted after upgrading.

Specifically, you need to reboot the following host servers after upgrading them to the current CA DLP version:

- CMS
- Gateway servers
- Policy engines
- Event Import machines
- Remote Data Manager (RDM) machines
- Quarantine Manager machines
- iConsole application servers

Note: You do not need to reboot upgraded iConsole front-end web servers.

- File Scanning Agent servers

Note: You do not need to reboot machines hosting the FSA Remote Connector utility.

Default Policy for Imported or Scanned Files

In previous versions, CA DLP tried to determine the policy participant for scanned or imported files by mapping the host machine ID onto user address lists, and applying the Fallback User policy if no match was found. But in the current CA DLP version, policy engines apply the Default Policy for Files to scanned or imported files if no other means are available to determine the policy participant.

Upgrading the iConsole

Note the following issues when upgrading your iConsole.

More information:

- Manually Upgrade Standard Searches, Reports and Dashboards (see page 31)
- Respecify Customized Reports Based on Policy or Class (see page 31)
- Color Coding for Incident Rate By Policy Report (see page 32)
- Update Virtual Directory References in iConsole Bookmarks (see page 32)
- Drop-Down Recipient Lists in Compose Mail Dialog (see page 33)
- New Location For Custom iConsole Images (see page 33)
Manually Upgrade Standard Searches, Reports and Dashboards

The upgrade procedure for iConsole searches, reports and dashboard requires additional manual steps.

This is because setup.exe in the current release can only locate and upgrade Windows Installer Packages already installed. iConsole searches, reports and dashboards installed before r12.0 were not installed as part of a package and therefore cannot be identified by the normal CA DLP upgrade procedure.

The required upgrade procedure is summarized below.

To upgrade the iConsole standard searches, reports and dashboard
1. Migrate your old Orchestria registry keys.
2. Run Setup.exe on your CMS and iConsole servers to upgrade the core functionality.
3. Manually run reports.msi on the CMS and each iConsole server.
   Find reports.msi in the \Windows folder of your CA DLP distribution image.
   On the CMS, this will upgrade the database stored procedures and functions.
   On the application servers, this will upgrade the required XML and JS files.
   On the front-end Web servers, this will upgrade the help and JS files.

Respecify Customized Reports Based on Policy or Class

After upgrading your iConsole servers, you may need to respecify any customized versions of reports that show results by policy or class, such as the Incident Rate By Policy Report. (Here, a ‘customized’ report means any report that has been modified and saved by a reviewer in the iConsole Customize Report screen.) Specifically, you may need to re-select the policies or classes that you want the report to use.

This is because the iConsole Report screens now presents users with a different mechanism for selecting policies or classes. Previously, these screens used a different selection mechanism and any policy or class previously selected cannot be shown in the current report screens.

You only need to re-select policies or classes if, after upgrading, you attempt to run the customized report from the iConsole Report customize screen. If you run the report directly, you do not need to reselect them; any previously selected policies or classes are preserved in the underlying XML report definition and the report runs as expected.
**Color Coding for Incident Rate By Policy Report**

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

**Update Virtual Directory References in iConsole Bookmarks**

The virtual directory for iConsole front-end Web servers is incorporated into the target URL for iConsole users. In CA DLP 6.0, the default virtual directory was *orchestria*. In CA DLP r12.5, the default virtual directory changed to *cadlp*.

If you deleted your version 6.0 iConsole installation before upgrading to the current version, any existing iConsole bookmarks (more commonly called 'favorites' in Internet Explorer) no longer work because their URLs still use the old virtual directory name. Therefore, you must update the URLs for your saved iConsole bookmarks to use the *cadlp* virtual directory.

**Note:** If you directly upgraded your 6.0 iConsole servers directly to the current version, you do **not** need to run this script; your iConsole bookmarks will be updated automatically to use the *cadlp* virtual directory.

**To update your iConsole bookmarks to use the *cadlp* virtual directory**

1. Find the iConsole bookmark script, UpdateBookmarks.wsf in the \Support folder on your CA DLP distribution media.
2. Do one of the following:
   - Run this command to replace 'orchestria' references with 'cadlp' in your iConsole bookmarks:
     ```bash
     UpdateBookmarks.wsf
     ```
   - Run this command to replace a customized virtual directory name with 'cadlp' in your iConsole bookmarks:
     ```bash
     UpdateBookmarks.wsf /oldvdirname:"<VirtualDir>"
     ```
     where `<VirtualDir>` is the customized virtual directory name.
Drop-Down Recipient Lists in Compose Mail Dialog

In the iConsole Compose Mail dialog, when a reviewer starts typing an address in the To, Cc, or Bcc fields, the iConsole displays a drop-down list of all matching users in Active Directory.

Previously, the underlying method for generating this list was based on an LDAP lookup operation that queried the cn (Common Name) attribute in Active Directory. Now, the LDAP lookup operation now queries the displayName attribute.

In most case, customers upgrading to the current CA DLP version will be unlikely to notice this subtle behavior change. But if required, you can specify which Active Directory attribute is used to populate the drop-down address lists. To do this, you edit the registry on your iConsole front-end Web servers. For details, see the Platform Deployment Guide; search for ‘iConsole: recipient lists’.

New Location For Custom iConsole Images

In the current CA DLP release, the folder containing these images for custom searches and reports has moved. These images are now stored in the CA DLP installation folder in the following subfolder:

\Web\images\dlp\main\standard\SDIcons

If you have custom iConsole searches or reports that predate r12.5 and which use custom images, you must:

1. Move these images to the \SDIcons subfolder.
2. Remove the image path from the XML search definition file.

Note: If the image path is currently set to ".\Web" or "\Web\images" in the XML search definition file, step 2 is not needed. The iConsole will be able to locate your custom images.
Dashboards

Previously, the dashboard was based on aggregated data held in database summary tables. Since CA DLP 14.0, the iConsole dashboard has been based on data held in the CA DLP data warehouse. The data warehouse is a set of database tables containing CA DLP 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 DLP 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 DLP.

Before CA DLP 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 DLP, 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 DLP 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.
Upgrading FSA Jobs

After upgrading your FSA server from version 6.0, you must upgrade any existing scanning jobs.

In CA DLP r12.0, the underlying XML schema for scanning job definition files was amended. If you have scanning jobs defined using a version 6.0 FSA, you must first import these jobs onto the upgraded FSA before you can run them. When you import 6.0 scanning jobs, the FSA automatically updates them to use the new job schema introduced in r12.0. You can then run these jobs as normal.

To upgrade 6.0 scanning jobs

1. Upgrade your FSA server. You must also install a current version Administration console.
2. In the FSA screen of the Administration console, select an FSA server and choose Edit > Import Job File.
3. This launches the Import FSA Job Definitions dialog. Browse to the XML job file that you want to import.
4. Each individual job defined in the 6.0 job file is added to the FSA screen.

   Note: If the 6.0 job file contained multiple scanning job definitions, the FSA creates a separate job file for each individual job extracted from the 6.0 job file.
Review Queue

(Only required if upgrading a SQL Server CMS)

In r12.0, the database views used by the Review Queue on SQL Server CMSs were renamed to make them consistent with the corresponding views on Oracle CMSs. (In version 6.0, an inconsistent naming convention was introduced inadvertently.)

Consequently, if you upgrade your SQL Server CMS to the current version but retain your version 6.0 Review Queue search (that is, you do not install the current version Review Queue search), then your existing 6.0 search will no longer run. To fix this problem, you must:

- **Either** install the current version Review Queue search and reports.
- **Or** add backwards compatibility between the current version of CA DLP and your existing 6.0 Review Queue search. To do this, run the script:
  
  `RQ_R11_Compat_Views_Wrapper.sql`.

  Briefly, this script re-creates the database views used by your 6.0 search so that they point to the new (renamed) database views used by the current version Review Queue search. When you upgrade your CMS, this script is installed to the CA DLP installation folder, in the following subfolder:

  `\CA\CA DLP\system\scripts\MSSQL\RQ`

  To run this script from the \system folder, the command syntax is:

  `wgninfra -exec wigan/schema/SchemaRunScript scripts\MSSQL\RQ\RQ_R11_Compat_Views_Wrapper.sql`

Log Files Are Not Relocated

In the current CA DLP release, log files are typically saved in CA's `\data\log` subfolder. On 32-bit machines, find this subfolder in the Windows All Users profile. On 64-bit machines, find this subfolder below the `\ProgramData` folder. See the *Platform Deployment Guide* for details.

However, when you upgrade from version 6.0, existing CA DLP log files are not relocated but stay in their previous location, that is, a different subfolder of the Windows All Users profile:

`\All Users\Application Data\Orchestria\Active Policy Management\data\log`
Chapter 5: Upgrading from 12.0

Note the following issues when upgrading from r12.0 to the current CA DLP version.

This section contains the following topics:
- Reboot Your CA DLP Servers (see page 39)
- Security Models (see page 40)
- Upgrading the iConsole (see page 40)
- Dashboards (see page 41)
- Administrative Privilege Renamed (see page 43)
- Log Files Are Not Relocated (see page 44)
- FSA Remote Connector Upgrades on 64-bit Machines (see page 45)
- Change in AuthenticatedUserType Default Value for ICAP Agent (see page 46)

Reboot Your CA DLP Servers

Changes to the infrastructure in the current version of CA DLP mean that any servers running the CA DLP infrastructure must be rebooted after upgrading.

Specifically, you need to reboot the following host servers after upgrading them to the current CA DLP version:
- CMS
- Gateway servers
- Policy engines
- Event Import machines
- Remote Data Manager (RDM) machines
- Quarantine Manager machines
- iConsole application servers

  Note: You do not need to reboot upgraded iConsole front-end web servers.

- File Scanning Agent servers

  Note: You do not need to reboot machines hosting the FSA Remote Connector utility.
Security Models

In the current CA DLP version, support for database security security models has been extended and managing security models has been simplified.

Note: In previous versions, database security models were referred to as Row Level Security (RLS) models.

Policy-based Security Model

CA DLP now supports an additional model based on policy classes and ensures that reviewers can only see specific types of event.

Support for Multiple Database Models

CA DLP now permits multiple database models to be active at the same time on the CMS. These models include the original model based on management groups, the new policy-based model, plus variants and hybrids of these models. Previously, you could only have one security model active at any time.

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

Security Models Managed in the Administration Console

You configure database models in the Administration console. Previously, you had to run RLS customization scripts to change the active security model. See the Database Guide for details; search for ‘security models’.

Upgrading the iConsole

Note the following issues when upgrading your iConsole.

More information:

Color Coding for Incident Rate By Policy Report (see page 40)
New Location For Custom iConsole Images (see page 41)

Color Coding for Incident Rate By Policy Report

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

In the current CA DLP release, the folder containing these images for custom searches and reports has moved. These images are now stored in the CA DLP installation folder in the following subfolder:

\Web\images\dlp\main\standard\SDIcons

If you have custom iConsole searches or reports that predate r12.5 and which use custom images, you must:

1. Move these images to the SDIcons subfolder.
2. Remove the image path from the XML search definition file.

Note: If the image path is currently set to "..Web" or "..\Web\images" in the XML search definition file, step 2 is not needed. The iConsole will be able to locate your custom images.

Dashboards

Previously, the dashboard was based on aggregated data held in database summary tables. Since CA DLP 14.0, the iConsole dashboard has been based on data held in the CA DLP data warehouse. The data warehouse is a set of database tables containing CA DLP 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 42)
Historical Dashboard Data is Lost After Upgrade (see page 43)
Delay Before the Dashboard is Updated

When you upgrade an iConsole dashboard to the current CA DLP 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 DLP.

Before CA DLP 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 DLP, 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 DLP 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.

Administrative Privilege Renamed

In the current CA DLP release, the privilege previously named 'Admin: Disable Management Group Filtering' has been renamed to 'Admin: Disable Security Model Filtering'.

This name change was introduced to more accurately reflect the wider scope of this privilege. The current release supports a significantly wider range of database security models. In previous releases, CA DLP only supported security models based on the CA DLP user hierarchy and management groups. Now, CA DLP supports additional security models based on policy classes.

This name change is handled automatically when upgrading your CMS. That is, any user accounts that previously had the 'Admin: Disable Management Group Filtering' privilege will, after upgrading, have the 'Admin: Disable Security Model Filtering' instead.
Log Files Are Not Relocated

In the current CA DLP release, log files are typically saved in CA's `\data\log` subfolder. On 32-bit machines, find this subfolder in the Windows All Users profile. On 64-bit machines, find this subfolder below the `\ProgramData` folder. See the Platform Deployment Guide for details.

If your r12.0 installation was a new deployment (not an upgrade from an earlier version), then the CA DLP log files will already be in CA's `\data\log` subfolder of the Windows All Users profile.

But if your r12.0 installation had been previously upgraded from version 5.0 or 6.0, then the existing log files are not relocated but will stay in their previous location: `\Program Files\Orchestria\Active Policy Management\system\data\log`
FSA Remote Connector Upgrades on 64-bit Machines

If you have an r12.0 FSA Remote Connector running on 64-bit Windows machines, note the following upgrade procedures.

To upgrade the FSA Remote Connector on 64-bit Windows machines

1. Run Integration_x64.msi or Setup.exe on the FSA Remote Connector host machine.
   Because of incompatibilities with the 32-bit FSA Remote Connector and the 64-bit upgraded version, this operation will uninstall the CA DLP Remote File Scanning Agent Connector service. This is expected behavior.
   Important! If upgrading the FSA Remote Connector on a 64-bit Windows that is hosting a 32-bit SharePoint server, see the following section for an alternative upgrade procedure.

2. Using Add/Remove Programs, choose Change, Repair to repair the FSA Remote Connector and complete the upgrade.
   This repair operation re-installs the CA DLP Remote File Scanning Agent Connector service.

FSA Remote Connector and 32-bit SharePoint Server on 64-bit Windows machines

If you have a 32-bit SharePoint server and a r12.0 FSA Remote Connector running on a 64-bit Windows machine, you must run Integration.msi on the host machine to upgrade the FSA Remote Connector. No further steps are necessary.

Integration.msi is a 32-bit installation package. You must use this package to upgrade because the bitness of the FSA Remote Connector must match the bitness of SharePoint.

- If an r12.0 FSA Remote Connector is installed on a 32-bit Sharepoint installation on 64-bit Windows, use the integration.msi 32-bit package. Do not use the integration_x64.msi package.
Change in AuthenticatedUserType Default Value for ICAP Agent

In the current CA DLP 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 DLP 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.
Chapter 6: Upgrading from 12.5

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

This section contains the following topics:

Dashboards (see page 47)
Color Coding for Incident Rate By Policy Report (see page 49)
Change in AuthenticatedUserType Default Value for ICAP Agent (see page 50)

Dashboards

Previously, the dashboard was based on aggregated data held in database summary tables. Since CA DLP 14.0, the iConsole dashboard has been based on data held in the CA DLP data warehouse. The data warehouse is a set of database tables containing CA DLP 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 48)
Historical Dashboard Data is Lost After Upgrade (see page 49)
Delay Before the Dashboard is Updated

When you upgrade an iConsole dashboard to the current CA DLP 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 DLP.

Before CA DLP 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 DLP, 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 DLP 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.

Color Coding for Incident Rate By Policy Report

In the current CA DLP release, it is no longer possible to customize the iConsole look-and-feel by editing styles in branded.css to override the base stylesheet.
Change in AuthenticatedUserType Default Value for ICAP Agent

In the current CA DLP 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 DLP 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.
Chapter 7: Upgrading Databases

This chapter describes the database issues associated with upgrading your CMS. Note the following issues if upgrading from version 6.0:

**CMS upgrades from 6.0 require database schema change**

In r12.0, some schema changes were made to the Wgn3EventParticipant database table to accommodate changes to security model handling.

Consequently, if upgrading from versions that predate r12.0, you must run a ‘pre-flight check’ before upgrading your CMS to estimate how long the database changes will take.

After upgrading your CMS, you also need to make a manual change to the Wgn3EventParticipant table.

This section contains the following topics:

- Database Schema Changes (see page 52)
- Pre-upgrade Database Considerations (see page 52)
- Upgrading a Partitioned Oracle Database (see page 54)
- Upgrading a 6.0 Database (see page 63)
- Enabling the Data Warehouse (see page 78)
Database Schema Changes

If you are upgrading your CA DLP servers to 14.0, note the following changes to the database schema.

For the current version of CA DLP, the database schema version is 3.70. This version includes various changes to support internationalization of the CA DLP product, faster search and report performance, and CA DLP integration with [assign the value for boe in your book].

New Tables and Related Indexes

WGN3ClassificationBASE
  WGN3ClassificationBASE.PK_WGN3ClassificationBASE
WGNWellKnownStringBASE
  WGNWellKnownStringBASE.PK_WGNWellKnownStringBase
WGN3StringI18N
  WGN3StringI18N.PK_WGN3StringI18N

Performance Optimizations

Wgn3Event Table
  New column: QueryFlags
  New Index: IX_Wgn3Event_QueryFlags

Wgn3EventParticipant Table
  New column: QueryFlags
  New Index: IX_Wgn3EventParty_QueryFlags

Role
  WGNReportingUser

Note: Full schema details are available in the CA DLP 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 53)
Oracle Issues (see page 53)
Database Schema Change (see page 54)

Back Up Your CMS Database Before Upgrading

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

Oracle Issues

Be aware of the following issues:

Oracle 9i not supported

Important! If upgrading from version 6.0, be aware that Oracle 9i is no longer supported.

If your existing CMS has an Oracle 9i database, you must upgrade to Oracle 10g or 11g before you can upgrade your CMS.

Oracle users need extra privileges

Before upgrading your CMS, you may need to manually grant extra privileges to your Oracle primary user and, if specified, the schema owner:

If upgrading from 12.0, you must grant:

- CREATE MATERIALIZED VIEW

If upgrading from 6.0, you must grant:

- CREATE JOB
- CREATE MATERIALIZED VIEW
- EXECUTE ON DBMS_LOCK
- SELECT ANY DICTIONARY

For a full list of required privileges, see the Database Guide; search the index for ‘privileges’.
Database Schema Change

Only required if upgrading from version 6.0

In r12.0, schema changes were made to the Wgn3EventParticipant database table to accommodate changes to security model handling.

Consequently, if upgrading from version 6.0, you must run a ‘pre-flight check’ before upgrading your CMS to estimate how long the database changes will take.

Upgrading a Partitioned Oracle Database

For upgrades from r12.0, you can choose a semi-automated database upgrade method, or you can fully customize the database upgrade using Native Upgrade scripts provided by CA DLP.

If upgrading from version 6.0, you must first upgrade your database to r12.0 and then upgrade to the current version of CA DLP.

More information:

- Semi-automated Database Upgrades (see page 55)
- Native Upgrade Scripts (see page 56)
- Native Script Upgrades from 6.0 (see page 57)
- Native Script Upgrades from r12.0 (see page 59)
- Upgrading from r12.5 (see page 62)
Semi-automated Database Upgrades

(Appplies to upgrades from 12.0 or later)

If your database partitioning scheme follows the CA DLP default configuration (in terms of naming conventions, the MAXVALUE partition, tablespace, and so on), you can upgrade your Oracle CMS by running the CA DLP 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.

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 DLP distribution image.
   CA DLP 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
Native Upgrade Scripts

CA DLP 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.

Find these scripts in the CA DLP distribution image, in 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.

\UpgradeV6_0ToV12_0
  The scripts in this folder are needed if you are upgrading a 6.0 CMS where you need to customize physical attributes of objects in the upgrade.

\UpgradeV12_0ToV12_5
  The scripts in this folder are needed 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. If upgrading from 6.0, these scripts comprise the second stage in the pre-upgrade process.

  **Note:** After upgrading from r12.0, you must run a table partitioning stored procedure (see page 61).

\UpgradeV12_5ToV14_0
  The scripts in this folder are needed 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:
  - 6.0, these scripts comprise the third stage in the pre-upgrade process.
  - r12.0, these scripts comprise the second stage in the pre-upgrade process.
Native Script Upgrades from 6.0

These instructions upgrade your CA DLP database from 6.0 to r12.0.

To upgrade from 6.0

1. Go to the \UpgradeV6_0ToV12_0 subfolder:

2. Copy this subfolder to your database host server (this is not necessarily the same as the CMS host server).

   This subfolder includes Native_UpgradeToVer3_50.sql and Native_Wrapper.sql.

3. Edit Native_UpgradeToVer3_50.sql on your database host server to make the changes you require.

   In particular, you may want to specify the tablespace and storage parameters for these new objects:

   **Captured Data Table**

   Wgn3ReviewQueue

   **Note:** By default for new CA DLP installations, this table is assigned to the WGNDATA tablespace.

   **Capture Data Indexes**

   IX_Wgn3ReviewQueue_Group
   IX_Wgn3ReviewQueue_User

   **Note:** By default for new CA DLP installations, these indexes are assigned to the WGNDATAIDX tablespace.

   **Other Data Tables**

   Wgn3JobHistory
   Wgn3JobState
   Wgn3UserAddressEx
   Wgn3ReviewMetrics
   Wgn3RTReviewMetrics
   Wgn3RTReviewTotals
   Wgn3RTReviewQueue
   Wgn3RTEventSlice

   **Note:** By default for new CA DLP installations, these tables are assigned to the WGN tablespace.

   **Other Data Indexes (WGNIDX)**

   PK_Wgn3JobHistory
   PK_Wgn3UserAddressEx
IX_Wgn3UserAddrEx UserID
PK_Wgn3ReviewMetrics
IX_Wgn3RTReviewTotals_Group
IX_Wgn3RTReviewQueue_Group
IX_WGN3RTEventSlice_Group

**Note:** By default for new CA DLP installations, these indexes are assigned to the WGNIDX tablespace.

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. You now need to upgrade from r12.0; see the next section.
Native Script Upgrades from r12.0

These instructions upgrade your CA DLP database from 12.0 to 12.5.

If your database partitioning scheme follows the CA DLP default configuration, you can use the semi-automated upgrade method. If you require more control and flexibility in managing your Oracle database, use the Native Upgrade scripts to upgrade. In both cases, you must run a stored procedure after upgrading your CMS.

To run a semi-automated upgrade
1. Upgrade the CMS by running setup.exe.
   Find this in the root of your CA DLP distribution image.
   The CA DLP database is upgraded accordingly, and includes the changes described in the section, 'Semi-automated Database Upgrades'.
2. Run the following command as the schema owner, using the SQL*Plus utility:
   ```sql
   EXEC WGN_PARTITION_UTIL.WGN_PARTITION_12_5_TABLES;
   ```
   Applying this stored procedure ensures that the Wgn3IssueTrigger table matches your existing partitioning scheme.

To upgrade using the native upgrade scripts
1. Go to the \UpgradeV12_0ToV12_5 subfolder in your CA DLP distribution image.
2. Copy this subfolder to your database host server.
   This subfolder includes Native_UpgradeToVer3_60.sql and Native_Wrapper.sql.
3. Edit Native_UpgradeToVer3_60.sql on your database host server to make the changes you require.
   In particular, you may want to specify the tablespace and storage parameters for these new objects:

   **Captured Data Index**
   ```sql
   IX_Wgn3Trigger_PolicyID
   ```
   **Note:** By default for new CA DLP installations, this index is assigned to the WGNDATAIDX tablespace.

   **Audit Data Table**
   ```sql
   Wgn3IssueTrigger
   ```
   **Note:** By default for new CA DLP installations, this table is assigned to the WGNDATA tablespace.

   **Audit Data Indexes**
   ```sql
   PK_Wgn3IssueTrigger
   IX_Wgn3IssueTrigger_Trigger
   ```

   [Page 59] Chapter 7: Upgrading Databases
Note: By default for new CA DLP installations, these indexes are assigned to the WGNDATAIDX tablespace.

Other Tables
- Wgn3Role
- Wgn3ResourceType
- Wgn3Resource
- Wgn3ResourceRole
- Wgn3UserRole

Note: By default for new CA DLP installations, these tables are assigned to the WGN tablespace.

Other Indexes
- IX_Wgn3UserDateGroup
- IX_WGN3GroupUpdateUser
- PK_Wgn3Role
- UK_Wgn3Role_Name
- IX_Wgn3Role_Parent
- PK_Wgn3ResourceType
- UK_Wgn3ResourceType_Class
- PK_Wgn3ResourceIX_Wgn3Resource_Policy
- IX_Wgn3Resource_ResourceType
- PK_Wgn3ResourceRole
- IX_Wgn3ResourceRole_Resource
- PK_Wgn3UserRole
- IX_Wgn3UserRole_User

Note: By default for new CA DLP installations, these indexes are assigned to the WGNIDX tablespace.

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 CMS by running setup.exe.

   Find this in the root of your CA DLP distribution image.
The CA DLP database is upgraded accordingly, and includes the changes described in the section, 'Semi-automated Database Upgrades'.

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

   EXEC WGN_PARTITION_UTIL.WGN_PARTITION_12_5_TABLES;

   Applying this stored procedure ensures that the Wgn3IssueTrigger table matches your existing partitioning scheme.

7. You now need to upgrade from r12.5; see the next section.

More information:

Semi-automated Database Upgrades (see page 55)
Table Partitioning SP (see page 61)

Table Partitioning SP

After upgrading your CMS from 12.0 (using setup.exe), you must manually 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 is installed when you upgrade your CMS by running setup.exe. It is called:

WGN_PARTITION_UTIL.WGN_PARTITION_12_5_TABLES

For full upgrade instructions, see the reference below.
Upgrading from r12.5

These instructions upgrade your CA DLP 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 DLP 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 DLP 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 DLP 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 );
Upgrading a 6.0 Database

(Only required if upgrading from version 6.0)

To accommodate changes to the default row level security model, some schema changes are needed for the Wgn3EventParticipant database table on the CMS. At the same time, any participant records in this table associated with Web and Application Monitor events must be updated.

Also, there is risk that some underlying historical data may be lost from incident trend charts when you upgrade your dashboard from 6.0 (see page 35).

More information:

What Database Changes Are Needed? (see page 63)
How to Upgrade a 6.0 Database (see page 64)
Oracle: Post-Upgrade Change To Event Participant Table (see page 67)
SQL Server: Post-Upgrade Change To Event Participant Table (see page 68)

What Database Changes Are Needed?

Since version 6.0, changes to the security model handling mean that every event participant in your CMS database must have an associated e-mail address. This particularly impacts participants in Web and Application Monitor events, for whom addresses were not previously stored.

Therefore, as part of the upgrade process, CA DLP assigns automatically-generated addresses to these participants. It then migrates all existing participant addresses, including these new ones, to the Wgn3UserAddressEx database table.

When the upgrade is complete, a final schema change is needed. Specifically, the database columns that identify participant addresses must be redefined as NOT NULL (participant address identifiers are now mandatory; previously, they were optional). This affects the AddressUID1 and AddressUID2 columns in the Wgn3EventParticipant table.

The schema change is the same for Oracle and SQL Server databases, but the implementation is more complex for SQL Server.
How to Upgrade a 6.0 Database

The upgrade procedure from 6.0, including pre- and post-upgrade tasks, is summarized in the following sections. Briefly, you must:

1. Run a pre-flight check script before you upgrade your CMS.
   This script estimates how long it will take to update the event participant records and migrate them to the new database table.

2. Upgrade your CMS.
   The upgrade will automatically update participant records to support the updated RLS model.

3. Run a script to edit the Wgn3EventParticipant database table after upgrading the CMS.
   Theis script redefines the AddressUID columns as NOT NULL to ensure that email addresses are mandatory for participants in this database table.

More information:

1. Run the Pre-Upgrade 'Participant Address' Pre-Flight Check (see page 65)
2. Upgrade the CMS (see page 65)
3. Modify the Event Participant Table (see page 66)
1. Run the Pre-Upgrade 'Participant Address' Pre-Flight Check

Before you upgrade your CMS, you must run a pre-flight check script, `wgn_pre_upgrade_pfc.sql`.

This script estimates how long it will take, as part of the CMS upgrade, to update the event participant records and migrate them to the new database table. The Oracle pre-flight check also estimates how long the post-upgrade changes to the Wgn3EventParticipant database table will take. You can use these estimates to plan your CMS upgrade. To run `wgn_pre_upgrade_pfc.sql`:

**SQL Server**

Find this script in the following folder on your CA DLP distribution media:

\Support\Upgrade12\MSQL

Open and execute this file in SQL Server Management Studio. To do this, use a login with the sysadmin role (for example, sa).

**Oracle**

Find this script in the following folder on your CA DLP distribution media:

\Support\Upgrade12\Oracle

Then, using SQL Plus connect to the CA DLP database as the CA DLP schema owner (typically APMOWNER on version 6.0 CMSs) and run this command:

`@wgn_pre_upgrade_pfc`

2. Upgrade the CMS

**Important!** We strongly recommend that you back up your database before you upgrade your CMS.

Upgrade your CMS as described elsewhere. Do this during a period of minimal user activity (typically, out of office hours).

The upgrade will automatically update participant records to support the updated RLS model. In technical terms, CA DLP assigns an AddressUID to any participant with a null address and then migrates all participant addresses to the Wgn3UserAddressEx database table.

**Note:** If upgrading a partitioned Oracle CMS, you must follow an amended upgrade procedure based on Native_Wrapper.sql scripts (these allow DBAs to use their own tablespace and partition naming conventions).
3. Modify the Event Participant Table

After upgrading the CMS, the AddressUID columns in the Wgn3EventParticipant database table must be redefined as NOT NULL. This ensures that email addresses are mandatory for participants in this database table. You must make this table change manually on the CMS (for gateways and other CA DLP servers, the table is modified automatically as part of the r12.0 upgrade).

- **For Oracle CMSs**, this is a simple schema change. Before you run the table update script, we recommend that you run a further pre-flight check script to estimate how long the table updates will take.

- **For SQL Server**, the process is more complicated. This is necessary for performance reasons. Our testing revealed that, paradoxically, a simple schema change such as that implemented for Oracle databases could be unacceptably slow and consume excessive disk space (for log files) when applied to very large SQL Server tables.

  Before you run the table update script, you must run a further pre-flight check script to check that the necessary system conditions are in place and to estimate how long the table updates will take and how much free disk space is required.

**More information:**

- Oracle: Post-Upgrade Change To Event Participant Table (see page 67)
- SQL Server: Post-Upgrade Change To Event Participant Table (see page 68)
Oracle: Post-Upgrade Change To Event Participant Table

(Only required if upgrading from version 6.0)

After upgrading your CMS, you need to modify the Wgn3EventParticipant table, redefining the AddressUID columns as NOT NULL.

To redefine the AddressUID columns

1. Run the pre-flight check script, wgn_post_upgrade_pfc.sql. This script estimates how long the table update will take.
   
   Find this script in the \Support\Upgrade12\Oracle folder on your CA DLP distribution media.
   
   Using SQL Plus, connect to the CA DLP database and run this command as the CA DLP schema owner (typically APMOWNER on version 6.0 CMSs):
   
   @wgn_post_upgrade_pfc

2. Run the wgn_common_upgrade_22b.sql to modify the Wgn3EventParticipant table.
   
   Find this script on your CMS in the \System\Scripts\Oracle subfolder of CA DLP installation folder:
   
   Using SQL Plus, run this script as the CA DLP schema owner (typically APMOWNER on version 6.0 CMSs):
   
   @wgn_common_upgrade_22b

3. Back up your database again to create a new restore point.
SQL Server: Post-Upgrade Change To Event Participant Table

(Only required if upgrading from version 6.0)

After upgrading your CMS, you must: run a pre-flight check; back up your CMS database; then run a script to modify the participant address columns in the Wgn3EventParticipant table. The full procedure is summarized below.

How to Implement the Post-Upgrade Table Change

1. Run a post-upgrade pre-flight check to confirm that the necessary conditions and requirements are met.
2. Back up your CMS.
3. Install the required stored procedures into your database.
4. Prepare to modify the table (for example, by restricting database access).
5. Run the 'modify table' script.
   
   You can run a single script that performs all the necessary steps, or you can run two separate scripts.
   
   Running two scripts allows you to check that preparations completed successfully before you truncate the table. (The bcp export log and script output indicate if any problems occurred during the preparations.)

   The actual table changes involve the following steps.
   a. Participant records are copied out of the table to a file.
   b. The table is truncated. This is why you must back up your CMS in step 2.
   c. The participant columns are redefined as mandatory.
   d. Participant records are copied back into the updated table.
6. Monitor the progress of table changes and confirm that the script has completed successfully. Progress is recorded in log files.
7. Verify that the table changes completed successfully.
8. Back up your CMS again to create a restore point.

These steps are described in the following sections.
1. Run the Post-Upgrade Pre-Flight Check

Before you actually update the Wgn3EventParticipant table so that it does not accept null Address UIDs, you must run a post-upgrade pre-flight check script. (Do not confuse this pre-flight check with the post-upgrade pre-flight check! (see page 65)) This post-upgrade pre-flight check is standalone and only exercises a small data export test. It does not update any data in the database.

We strongly recommend that you run the pre-flight check one or two days before the actual database upgrade. This gives you time to fix any problems uncovered by the script without disrupting your upgrade schedule.

What Does the Pre-Flight Check Do?

The pre-flight check script:

- Verifies that all required permissions are set (for example, bcp permission to write to the target directory).
- Verifies that the target folder exists.
- Verifies that sufficient free disk space is available in the target folder.

The pre-flight check also estimates how long the table updates will take. The time estimate is based on a sample of one million table rows. Using the 'bcp' utility, the pre-flight check script copies a maximum of one million rows from the table to the file system, measuring the time and disk space required to do so. Using these figures, it then calculates the disk space required to copy out the entire table and estimates how long this will take.

To run the pre-flight check.

1. Locate the pre-flight check file in your CA DLP distribution media.
   - The post-upgrade pre-flight check is implemented as a stored procedure (SP), contained in the following file:
     - wgn_post_upgrade_pfc.sql
   - Find this file in the following folder:
     - \Support\Upgrade12\MSSQL
2. In SQL Server Management Studio, open and execute this file to create the SP.

3. Run the following command as a login with the sysadmin role (we recommend sa). Note that you must use the same login when you actually modify the table (see step 1 in section 4, Run the Modify Table Script).

   ```sql
   EXEC dbo.wgn_post_upgrade_pfc '<dir>'
   ```

   where `<dir>` is the target folder where participant records will be copied to. You must specify a folder on the database host server (this is not necessarily the same as the CMS host server). This folder must already exist. For example:

   ```sql
   EXEC dbo.wgn_post_upgrade_pfc '\unxsvr1\participants\MyFolder'
   ```

   **Important:** Note the following requirements for the target folder!

   - Specify the target folder as a local path or UNC path. You cannot specify a mapped network drive letter (such as 'Z:\MyDrive').
   - Do not include a trailing backslash.
   - If the target folder is on a clustered SQL Server system, this folder must exist on all cluster nodes.
   - The Windows account that xp_cmdshell runs as must have Read/Write access to this folder.
     
     If xp_cmdshell runs as the SQL admin user, this account is the MSSQL service account.
     
     If xp_cmdshell runs as a different user, this account is the configured `##xp_cmdshell_proxy_account##`.
   - You must specify the same target folder for the pre-flight check and the actual table update. This ensures that the time estimate, permissions check, and disk space check are meaningful.
   - For performance reasons, we strongly recommend that this directory is on a separate disk from the actual database.
4. Check the script output in the Messages pane in SQL Server Management Studio.

   **Note:** By default, the Results pane displays. Switch to the Messages pane to view the output.

   This output indicates whether the necessary conditions have been met and estimates the time needed to update the table. In particular, the script output:
   - Confirms whether the AddressUID columns are currently defined as NULL.
   - Confirms whether the xp_cmdshell feature is enabled and the specified login has permission to use it. The table modification script will use this feature to run bcp commands when copying participant records between the database and the target directory.
   - Shows the actual bcp command used by the pre-flight check to copy table records to the target directory. To help diagnose problems, the bcp output is also piped to a log file, bcp_pf_ep_data.log.
   - Indicates whether there is sufficient free disk space in the target directory to store all the participant records.
   - Estimates how long the entire procedure will take to modify the Wgn3EventParticipant table, or the script indicates that bcp command failed.

**More information:**

- Pre-Flight Check Output (see page 71)
- Example 1: Pre-Flight Check All OK (see page 72)
- Example 2 Pre-Flight Check: CHECK Failed (see page 73)

**Pre-Flight Check Output**

When you run the post-upgrade pre-flight check the output indicates whether the necessary conditions have been met and estimates the time needed to update the table (see step 2 in 'Run the Pre-Flight Check').

The following sections show two example outputs. Example 1 indicates that all necessary conditions are OK and that the target directory for database records is C:\DBUpgrade. Conversely, example 2 indicates an invalid condition. In this example, the user has specified a non-existent target directory, C:\DBUpgradw.
Example 1: Pre-Flight Check All OK

In this example, the script output indicates all necessary conditions are OK. You can proceed with the table update.

```
**********************************************************************
*** Pre-flight Check has started
**********************************************************************

Participant address columns:
OK: Wgn3EventParticipant.addressuid1 is currently defined as optional
OK: Wgn3EventParticipant.addressuid2 is currently defined as optional

xp_cmdshell and BCP utility:
OK: xp_cmdshell is enabled on this server
OK: xp_cmdshell will run under this database account
OK: BCP successfully wrote to C:\DBUpgradedata\bcp_pf_ep_data.txt

Free disk space:
OK: Available disk space in C:\DBUpgradedata exceeds required disk space
Available disk space: 2933 Mb
Required disk space: 1 Mb

Time estimate:
Total time required to modify Wgn3EventParticipant table: 2800mS
This is our best estimate of how long it will take to upgrade your database.
Please allow for this when planning your CMS upgrade.

bcp command:
This Pre-flight Check uses this command to copy database records
to bcp pf ep data.txt.
For diagnostic purposes, the output is piped to bcp_pf ep data.log.bcp.
"SELECT TOP 432 * FROM [WGN_TA-RL-WS2].dbo.Wgn3EventParticipant"
queryout C:\DBUpgrade\bcp_pf_ep_data.txt -N -S "TA-RL-XP"
-T >C:\DBUpgrade\bcp_pf_ep_data.txt

**********************************************************************
*** Pre-flight Check is complete
**********************************************************************
```
Example 2 Pre-Flight Check: CHECK Failed

In this example, the bcp command failed because the target directory was mis-specified. You must fix this problem before you can proceed with the table update.

```
**********************************************************************
*** Pre-flight Check has started
**********************************************************************

Participant address columns:
OK: Wgn3EventParticipant.addressuid1 is currently defined as optional
OK: Wgn3EventParticipant.addressuid2 is currently defined as optional

xp_cmdshell and BCP utility:
OK: xp_cmdshell is enabled on this server
OK: xp_cmdshell will run under this database account

bcp command:
bcp "SELECT TOP 432 * FROM [WGN_TA-RL-WS2].dbo.Wgn3EventParticipant"
queryout C:\DBUpgradw\bcp_pf_ep_data.txt -N -S "TA-RL-XP"
-T >C:\DBUpgrade\bcp_pf_ep_data.log
Error: Pre-flight check aborted BCP failed to write to
C:\DBUpgradw\bcp_pf_ep_data.txt with return code 1 Error Severity 18
Error state 1

**********************************************************************
*** Pre-flight Check has failed
**********************************************************************
```

2. Back up Your CMS Database

Back up your CMS database before modifying the Wgn3EventParticipant table. You must also back up your CMS after modifying the table to create a new restore point.

In particular, be aware that the database recovery model will be switched to BULK_LOGGED mode while the participant records are restored. As a consequence, any table backups that predate the modification will not be usable if you need to restore the table in the future.

More information:

5. Run the Modify Table Script (see page 75)
3. Install the SPs Into Your Database (see page 74)
3. Install the SPs Into Your Database

You must run a script to install the required SPs. This script is wgn_post_upgrade_install.sql. When you upgrade your CMS, this script is installed automatically into the \System\Scripts\MSSQL subfolder of the CA DLP installation folder.

To install the SPs into your database

1. Run the following DOS command on the CMS:
   wgninfra -exec wigan/schema/Schema
   RunScript \Scripts\MSSQL\wgn_post_upgrade_install.sql
   This script installs these SPs into the CMS database.
   wgn_post_upgrade.sql
   This script runs the entire post-upgrade table modification as a single procedure.
   wgn_post_upgrade_1.sql
   This script runs the first part of the post-upgrade table modification. It stops at the point where all participant records have been copied to a file and before the table is truncated.
   wgn_post_upgrade_2.sql
   This script runs the second part of the table modification. It resumes at the point where Wgn3EventParticipant is truncated. It then makes the necessary column changes, and copies the participant records back into the table.

2. Check the log files to verify that the installation was successful.

More information:

1. Run the Post-Upgrade Pre-Flight Check (see page 69)

4. Prepare to Modify the Table

Before you modify the participant address column definitions in the Wgn3EventParticipant table, verify that no changes, or attempted changes, can be made to the table while the update is in progress. You therefore need to:

1. Stop the CA DLP infrastructure service on the CMS. To do this, run the following command:
   net stop wgninfra
   Note: We recommend that you also disable the service temporarily to prevent it from restarting automatically.

2. Verify that no other users are logged onto the CMS database.
5. Run the Modify Table Script

The section describes how to modify the Wgn3EventParticipant table.

To modify Wgn3EventParticipant

1. Open a new SQL Server Management Studio query window and run one of the following commands as a user with the sysadmin role (we recommend sa). This must be the same user that you used to run the pre-flight check (see step 2 in 'Run the Pre-Flight Check'):

   EXEC dbo.wgn_post_upgrade '<dir>'
   This command performs the entire table update as a single procedure. No further input is required.

   EXEC dbo.wgn_post_upgrade_1 '<dir>'
   This command runs part one of the table update, stopping at the point where all participant records have been copied to a file and Wgn3EventParticipant is ready to be truncated:
   
   Where <dir> is the target directory where the participant records will be copied to. In both cases, this must be the same folder that you specified in the pre-flight check script (step 2 in 'Run the Pre-Flight Check').

2. (Only applicable if you ran the ‘part one’ script in step 1). The script terminates after copying participant records to the file system (see below). This allows you to confirm that data has been copied out successfully and to perform other administrative tasks.

   For example, you may want to back up bcp_pf_ep_data.txt.

   Important! If you do back up bcp_pf_ep_data.txt, leave the original file in its current location so that it can be reloaded!

3. (Only applicable if you ran the ‘part one’ script in step 1). In SQL Server Management Studio, run the ‘part two’ script, using the same user that you used to run the ‘part one’ script:

   EXEC dbo.wgn_post_upgrade_2 '<dir>'
   Where <dir> is the same directory that you specified in step 1.

What Does the Script Do?

In technical terms, the script performs the following tasks.

1. Prepares the database

   The script takes preparatory steps to restrict access to the table and to enable the participant address columns to be redefined. In particular:

   - Access to the database is revoked for the CA DLP primary user.
   - The database is switched from ‘multi user’ to ‘single user’ mode.
- Relevant foreign key constraints and indexes on the Wgn3EventParticipant table are dropped or disabled.

2. **Copies participant records to the file system**
   a. First, the script changes the database from ‘single user’ to ‘restricted user’ mode. This enables the bcp utility to connect to the database.
   b. Next, it runs a bcp command to copy data out of the table to the `bcp_pf_ep_data.txt` file in the target directory. Progress is recorded in the `bcp_ep_out.log` log file.

3. **Truncates the table**
   This is the critical step! The script now truncates the Wgn3EventParticipant table, leaving it empty.

4. **Sets the AddressUID columns to NOT NULL**
   The script now makes the participant address columns mandatory.

5. **Copies participant records back into the table**
   a. First, the script sets the database recovery model to BULK_LOGGED mode. This eliminates the need to write Before and After images of each record to a log file during the copy operation.
   b. It then runs a bcp command to copy participant records from `bcp_pf_ep_data.txt` back into the Wgn3EventParticipant table. Progress is recorded in the `bcp_ep_in.log` log file.
   c. It verifies that the copy operation was successful, checking that the number of table rows copied out equals the number of rows copied in.

6. **Reverses the previous preparatory steps**
   Finally, the script reverses the earlier preparatory steps (see step 2). Specifically, it:
   - Sets the database from ‘restricted user’ mode back to ‘single user’ mode and then rebuilds any dropped indexes and re-enables any dropped foreign key constraints.
   - Sets the database from ‘single user’ mode back to ‘multi user’ mode.
   - Resets recovery model back to whatever it was before (FULL or SIMPLE).
   - Restores the ability of the CA DLP primary user to connect to the database.

**More information:**

1. Run the Post-Upgrade Pre-Flight Check (see page 69)
6. Monitor the Progress of Table Changes

(Available for SQL Server CMSs only)

CA DLP provides two levels of logging for the post-upgrade changes to the Wgn3EventParticipant table:

- First, each step in the overall procedure is recorded in the Wgn3JobState database table for diagnostic purposes. For example, entries are written to this table when a foreign key constraint is dropped (or re-enabled), or when the database is changed from ‘multi user’ to ‘single user’ mode.
- Second, for each bcp copy operation, progress is logged in the bcp_ep_out.log and bcp_ep_in.log files for each 1,000 rows copied into or out of the table. In addition, summary data at the end of the log file shows the total time to copy all the rows and the average rate at which they were copied.

7. Verify The Table Changes Completed Successfully

After the script completes the changes to the Wgn3EventParticipant table, verify from the script output and bcp logs that no errors occurred. In particular, verify that the participant count after the table change is the same as the count before the table change.

If the Table Changes Did Not Complete Successfully

Use any error messages to investigate and fix the cause. If you find a problem and are unsure how to continue, we recommend that you run the upgrade again. Start by restoring the CMS database from your back up. (This is why it is critical that you do make a backup!)

After you have restored the CMS from a backup and resolved the problem, you can repeat steps 3 through 7 of the post-upgrade table change process.

8. Back Up Your CMS Database Again

The table update is now complete. As a final step in the overall procedure, you now need to back up your CMS database again to create a new restore point.

This is not just good practice. It is an essential precautionary step because, while the table was being repopulated (see step 7 in section 5, Run the Modify Table Script), the database recovery model was set to BULK_LOGGED mode. Consequently, the changes to the participant records were not logged. This means that any table backups predating the post-upgrade changes to the participant address columns will not be usable if you need to restore the table in the future.
Enabling the Data Warehouse

The Data Warehouse is a set of database tables containing CA DLP event data that has been transformed into a format suitable for generating reports and iConsole dashboards. When you upgrade your CMS to the current version of CA DLP, the installer creates but does not enable the Data Warehouse.

How To Enable the Data Warehouse After Upgrading CA DLP

Enabling the Data Warehouse requires the following steps. You must perform these steps in the order listed below. Details are provided in the following sections.

1. Create the Data Warehouse User database account.
2. (Optional) Create the Unrestricted Search User database account.
3. Enable the Data Warehouse.
4. (Optional) Enable the Event Participant Fact table in the Data Warehouse.

More information:

Specify the Data Warehouse User (see page 79)
Specify the Unrestricted Search User (see page 80)
Manually Enable the Data Warehouse (see page 81)
Enable the Event Participant Fact Table (see page 81)
Specify the Data Warehouse User

Before you enable the Data Warehouse, you must specify the Data Warehouse User database account. External reporting applications (such as BusinessObjects Enterprise) use this database account to connect to the Data Warehouse and CMS database.

To specify an existing Data Warehouse User

Run the following command from a command prompt in the \system subfolder of the CA DLP installation folder on the CMS:

```
wgninfra -localexec wigan/schema/Schema SetUser Reporting <DWuser_Name> <DWuser_Password>
```

Where `<DWuser_Name>` and `<DWuser_Password>` specify the username and password for the Data Warehouse User database account.

To create and specify a new Data Warehouse User

If this database account does not already exist, you must create it. You can run a variation of the previous command to create the account and set this account to be the Data Warehouse User.

Run the following command from a command prompt in the \system subfolder of the CA DLP installation folder on the CMS:

```
wgninfra -localexec wigan/schema/Schema SetUser Reporting <DWuser_Name> <DWuser_Password> Create [<DBA_Name> <DBA_Password> <Tablespace>]
```

Where:

- `<DBA_Name>` and `<DBA_Password>` specify the username and password for a Database Administrator account that CA DLP can use to log in to SQL Server or Oracle to create the Data Warehouse User.
- `<Tablespace>` specifies the default tablespace for the Data Warehouse User.

**Important!** The tablespace parameter is only used by Oracle databases. However, you must always supply this parameter, even if the data warehouse is hosted in a SQL Server database. The SetUser command requires this parameter, even though the actual value is disregarded by SQL Server databases.

**Oracle Example**

The following command creates a Data Warehouse User named `WgnDWUser` with a password of `DWq74gsr`. The command assigns the Data Warehouse User to the `Users` tablespace and specifies a DBA named `sa` with a password of `DBAzr94x`.

```
wgninfra -localexec wigan/schema/Schema SetUser Reporting WgnDWUser DWq74gsr Create sys DBAzr94x Users
```

**SQL Server Example**
The following command creates a Data Warehouse User named *WgnDWUser* with a password of *(DWyu8b1s)*. The command specifies a DBA named *sys* with a password of *(DBAd23cz)*. The command includes a tablespace parameter (set to *null*) to satisfy the SetUser syntax requirements, even though SQL Server databases disregard this parameter.

```
wgninfra -localexec wigan/schema/Schema SetUser Reporting WgnDWUser DWyu8b1s Create sa DBAd23cz null
```

**Specify 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 DLP consoles and external reporting tools can use this database account when searching the CA DLP 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.

**To specify an existing Unrestricted Search User**

From a command prompt in the \system subfolder of the CA DLP installation folder on the CMS, run the following command:

```
wgninfra -localexec wigan/schema/Schema SetUser Unrestricted <Username> <Password>
```

Where <Username> and <Password> specify the username and password for the database account.

**To create and specify the Unrestricted Search User**

If this database account does not already exist, you must create it. If required, you can run a variation of the previous command to create a new database account and set this account to be the Unrestricted Search User.

From a command prompt in the \system subfolder of the CA DLP installation folder on the CMS, run the following command:

```
wgninfra -localexec wigan/schema/Schema SetUser Unrestricted <Username> <Password> [Create <dbAdminUserName>]```

Where <dbAdminUserName> specifies a Database Administrator User that CA DLP can use to log in to SQL Server or Oracle to create the new Unrestricted Search User.
Manually Enable the Data Warehouse

You manually enable the data warehouse by running a wgninfra.exe command. From a command prompt in the \system subfolder of the CA DLP installation folder on the CMS, run the following command:

```bash
wgninfra -localexec wigan/schema/Schema RunScript "scripts\DW\DWEnableDW.sql"
```

Enable the Event Participant Fact Table

The Event Participant Fact table in the Data Warehouse associates events with participants. When you enable this table, event participant data gets stored in the Data Warehouse.

You manually enable the Event Participant Fact table by running a wgninfra.exe command. You can also manually disable this table.

**Enable the Event Participant Fact table**

From a command prompt in the \system subfolder of the CA DLP installation folder on the CMS, run the following command:

```bash
wgninfra -localexec wigan/schema/Schema RunScript "scripts\DW\DWEnableEPFact.sql"
```

**Disable the Event Participant Fact table**

From a command prompt in the \system subfolder of the CA DLP installation folder on the CMS, run the following command:

```bash
wgninfra -localexec wigan/schema/Schema RunScript "scripts\DW\DWDisableEPFact.sql"
```

Do I Need To Collect Event Participant Data?

This section summarizes the issues to consider when deciding whether to enable or disable the Event Participant Fact table in the data warehouse.

The Data Warehouse installer includes a 'Collect event participant data' check box. This check box determines whether the Event Participant Fact table is enabled or disabled. This table in the Data Warehouse associates events with participants.

**If the Event Participant Fact table is enabled**

This table has the potential to grow very large. Our testing indicates that the table can increase the size of the CMS database by 30-40%. The reason is because an individual event can have many participants.

However, enabling the Event Participant Fact table has one important advantage. Namely, users assigned to a Management Group security model can successfully run BusinessObjects reports for CA DLP.
If the Event Participant Fact table is disabled

The BusinessObjects reports for CA DLP do not support filtering by user or user group. In turn, the reports do not support the Management Group security model. (Under this model, reviewers can only view events where at least one participant was in their management group when the event was captured.) Therefore, if users assigned to a Management Group security model run a BusinessObjects report for CA DLP, the report returns zero results.

Users assigned to a Policy security model can run these reports, but they cannot filter the reports by user or user group (even if users and groups are shown as configurable report parameters).

Users who only need the iConsole dashboard (but not the BusinessObjects reports for CA DLP) can leave the Event Participant Fact table disabled. The dashboard does not use data in this table.

Note: If you already use the iConsole dashboard but now want to start running BusinessObjects reports for CA DLP, you must enable and populate the Event Participant Fact. See the reference below for details.

Can I subsequently enable or disable the Event Participant Fact table?

Yes. You can manually enable or disable the Event Participant Fact table by running wgninfra.exe commands. See the following section for details.

Note: If you want to start running BusinessObjects reports for CA DLP, you must enable and populate the Event Participant Fact. It is not sufficient to simply enable this table. See the reference below for details.
Appendix A: Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are supported by CA DLP.

Display

To increase visibility on your computer display, you can adjust the following options:

**Font style, color, and size of items**
- Defines font color, size, and other visual combinations.
  - The CA DLP iConsole also supports a High Visibility mode. This increases the size of text and images in the iConsole screens.

**Screen resolution**
- Defines the pixel count to enlarge objects on the screen.

**Cursor width and blink rate**
- Defines the cursor width or blink rate, which makes the cursor easier to find or minimize its blinking.

**Icon size**
- Defines the size of icons. You can make icons larger for visibility or smaller for increased screen space.

**High contrast schemes**
- Defines color combinations. You can select colors that are easier to see.
Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

**Volume**
- Sets the computer sound up or down.

**Text-to-Speech**
- Sets the computer's hear command options and text read aloud.

**Warnings**
- Defines visual warnings.

**Notices**
- Defines the aural or visual cues when accessibility features are turned on or off.

**Schemes**
- Associates computer sounds with specific system events.

**Captions**
- Displays captions for speech and sounds.

Keyboard

You can make the following keyboard adjustments:

**Repeat Rate**
- Defines how quickly a character repeats when a key is struck.

**Tones**
- Defines tones when pressing certain keys.

**Sticky Keys**
- Defines the modifier key, such as Shift, Ctrl, Alt, or the Windows Logo key, for shortcut key combinations. Sticky keys remain active until another key is pressed.
Mouse

You can use the following options to make your mouse faster and easier to use:

**Click Speed**
Defines how fast to click the mouse button to make a selection.

**Click Lock**
Sets the mouse to highlight or drag without holding down the mouse button.

**Reverse Action**
Sets the reverse function controlled by the left and right mouse keys.

**Blink Rate**
Defines how fast the cursor blinks or if it blinks at all.

**Pointer Options**
Let you do the following:
- Hide the pointer while typing
- Show the location of the pointer
- Set the speed that the pointer moves on the screen
- Choose the pointer’s size and color for increased visibility
- Move the pointer to a default location in a dialog box
Index

6
6.0, upgrading from • 29

A
ASP.NET, for iConsole • 21

B
before upgrading • 19
bookmarks, for iConsole • 32

C
CMS • 21
back up and suspend • 21
Custom base policies • 14

D
database • 52
upgrade issues • 52

F
file compatibility • 11

I
iConsole • 21, 31, 32, 33
bookmarks, updating • 32
customized reports • 31
.NET Framework • 21
recipient lists • 33
virtual directories • 32

K
known issues when upgrading • 52
databases • 52

M
major and minor changes to policy schema • 13

N
.NET Framework, for iConsole • 21

P
policy compatibility • 11

post-upgrade tasks • 29
upgrading from 6.0 • 29
pre-flight checks • 65, 69, 71
after upgrading CMS • 69, 71
equal example output • 71
SQL Server • 69
before upgrading CMS • 65
pre-upgrade tasks • 19

R
reports for iConsole, need to respecify • 31
Review Queue • 37

U
Universal Adapter • 28

V
version compatibility • 11
virtual directory, for iConsole • 32