



Opsware® Data Center Intelligence 1.6 Guide

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.
T + 1 408.744.7300 F +1 408.744.7383 www.opsware.com

Copyright © 2000-2005 Opsware Inc. All Rights Reserved.

Opsware Inc. Unpublished Confidential Information. NOT for Redistribution. All Rights Reserved.

Opsware is protected by U.S. Patent Nos. 6,658,426, 6,751,702, 6,816,897, 6,763,361 and patents pending

Opsware, Opsware Command Center, Model Repository, Data Access Engine, Web Services Data Access Engine, Software Repository, Command Engine, Opsware Agent, Model Repository Multimaster Component, and Code Deployment & Rollback are trademarks and service marks of Opsware Inc. All other marks mentioned in this document are the property of their respective owners.

Additional proprietary information about third party and open source materials can be found at <http://www.opsware.com/support/opensourcedoc.pdf>.

Table of Contents

About This Guide	v
Contents of This Guide	v
About Opsware Documentation	vi
Conventions in This Guide	vi
Icons in This Guide	vi
Guides in the Documentation Set and Who Should Read Them	vii
Contacting Opsware, Inc.	viii
.....	viii
Chapter 1: Installing and Configuring the DCI Report Server	1
Prerequisites	1
Installing the DCI Report Server	5
Uninstall the Older Version of ISMTool	5
Install the ISMTool	6
Unpack and Upload the DCI Report Server Package	7
Set Custom Attributes Values on DCI Report Server Software Node ...	8
Install the DCI Report Server Software	10
Configuring DCI Report Servers in a Multimaster Mesh	11
Configuring a Single DCI Server in a Multimaster Mesh	12
Configuring Multiple DCI Servers in a Multimaster Mesh	13
Chapter 2: Uninstalling, Moving, Upgrading DCI	17
About Uninstalling, Moving, Upgrading DCI Report Server	17

Uninstalling the DCI Report Server	17
Moving DCI Report Server	19
Updating DCI Report Server in Multimaster Mesh	19
Upgrading the DCI Report Server.	19

Chapter 3: DCI Reports **21**

About DCI Reporting	21
Accessing DCI Reports in the OCC	21
Report Parameters	23
Report Results	25
Graphical View Report Results	26
List View Report Results	28
Individual Server Results View	29
Report Results Toolbar Buttons	29
DCI Reports	31
Server Reports	32
Network Reports	50
Compliance Center	59
Custom Reports	63
Ad-hoc Reports	63

Chapter 4: Writing Custom Reports **65**

Understanding Access to Public Views	65
Using a Shipped Report to Create a Custom Report	65
Extending Reports with other Data Sources	66
Installing a Customized Report	67
Using def.xml for Custom Reports	68

What is a def.xml file?	68
Layout of the def.xml file.	68
Backup and Restoration of Custom Reports.	69
Sample def.xml file	69

Chapter 5: DCI Report Server FAQ 73

How Do I Restart or Stop the DCI Report Server?	73
How Do I Change the DCI Username and/or Password?	73
How Do I Change the Public Views Password in Oracle?	74
How Do I Change the Public Views Password In DCI?	75
How Do I Keep the Public Views Password Secure?	76
What Time Zone is Used in Reporting?	77
Can I Share the DCI Report Server With Other Web Applications?	77

Chapter 6: Troubleshooting DCI Report Server 79

Troubleshooting General Errors In the DCI Report Server.	79
Step 1 - Did the DCI Package Upload?	79
Step 2 - Did the DCI Report Server Install?	79
Step 3 - Can You Access DCI in the OCC?	82
Step 4 - Can You View a Standard Report?	83
Step 5 - Do You See Any Custom Reports, And Are They Working?	84
Miscellaneous DCI Report Server Troubleshooting	84

Delay Occurs While Generating Some Server Reports.	85
Prompt for User Name/Password When Accessing DCI Home Page. . .	85
Database Login is Displayed When Running a Report	86
Microsoft VBScript Runtime Error	86
Running a Report Returns a Page Full of “unspecified errors”	86
Images and Graphs Missing on a Report.	87
A Report “hangs” for Longer Than Five Minutes.	87
Troubleshooting Windows Permissions for DCI	87
DCI User Not Created on Windows.	88
Error Seen on All Links in a Report.	88
Contacting Opware Support.	88

Preface

Welcome to Data Center Intelligence (DCI) Report Server. DCI Report Server reports provide real-time comprehensive information about an organizations servers, compliance, software, customers, operating systems, patches, compliance policies and what changes have occurred and should occur. After an action completes in the Opware Command Center, it is available in the DCI Reports.

About This Guide

This guide describes how to install, upgrade, uninstall, use, troubleshoot, and customize your DCI Reports, starting with instructions on how to install the DCI Report Server, followed by a chapter on how to uninstall, move, and upgrade the DCI Report Server. The next chapter explains how to use DCI Reports from the Opware Command Center (OCC) and describes all of the report results. The next chapter shows you how to write custom reports, followed by a FAQ of commonly asked questions and chapter on how to troubleshoot potential errors with the DCI Report Server.

This guide is intended for both system administrators who are responsible for all aspects of installing and configuring your DCI Report Server, and for end users who would like to generate and view DCI Reports.

Contents of This Guide

This guide contains the following chapters and appendices:

Chapter 1: Installing and Configuring DCI Report Server: Provides instructions on how to install and configure the DCI Report Server. This chapter included information on installing and configuring the DCI Report Server in a multimaster mesh environment.

Chapter 2: Uninstalling, Moving, and Upgrading DCI Report Server: Includes instructions on uninstalling, moving, and upgrading the DCI Report Server.

Chapter 3: DCI Reports: Explains how to generate DCI reports, how to understand the different types of report results, and explains what each of the reports mean.

Chapter 4: Writing Custom Reports: Provides information about configuring the Crystal Reports server in order to create your own custom reports with the DCI Report Server.

Chapter 5: DCI Report Server FAQ: Provides answers to frequently asked questions about the installation, configuration, and use of your DCI Report Server.

Chapter 6: Troubleshooting DCI Report Server: Includes information about how to troubleshoot and solve common problems and errors you might run into using the DCI Report Server.

About Opsware Documentation



Conventions in This Guide



This guide uses the following typographical and formatting conventions.

NOTATION	DESCRIPTION
<i>Courier</i>	Identifies text of displayed messages and other output from Opsware programs or tools.
Courier Bold	Identifies user-entered text (commands or information).
<i>Courier Italics</i>	Identifies variable user-entered text on the command line or within example files.

Icons in This Guide

This guide uses the following iconographic conventions.

ICON	DESCRIPTION
	This icon represents a note. It identifies especially important concepts that warrant added emphasis.
	This icon represents a requirement. It identifies a task that must be performed before an action under discussion can be performed.

ICON	DESCRIPTION
	<p>This icon represents a tip. It identifies information that can help simplify or clarify tasks.</p>
	<p>This icon represents a warning. It is used to identify significant information that must be read before proceeding.</p>

Guides in the Documentation Set and Who Should Read Them

- The *Opware[®] SAS 5.2 User's Guide* is intended to be read by the system administrator who is responsible for performing the day-to-day functions of managing servers, provisioning operating systems, uploading packages, setting up the Software Tree and node hierarchies, attaching software applications and installing them on servers, managing patches, reconciling servers with software, creating and executing scripts, tracking configuration, and deploying and rolling back code and content. It also documents the day-to-day functions of managing servers, such as server compliance and auditing, software packaging, application configuration, agent deployment, and global shell remote data center management.
- The *Opware[®] SAS 5.2 Administration Guide* is intended to be read by Opware administrators who will be responsible for setting up accounts for users, creating user groups and additional Opware administrators, assigning permissions for different levels of operation and access, adding customers and facilities, and monitoring and diagnosing the health of the Opware SAS components.
- The *Opware[®] SAS 5.2 Deployment and Installation Guide* is intended to be used by system administrators who are responsible for the installation of Opware SAS in a facility. It documents how to run the Opware Installer and how to configure each of the components.
- The *Planning Deployments for Opware[®] SAS 5.2* is intended to be used by advanced system administrators who will be responsible for planning all facets of an Opware SAS installation and deployment. It documents all the main features of Opware SAS and scopes out the planning tasks necessary to successfully deploy Opware SAS. Sections include: planning the Opware SAS design for a core, types of installations,

and discusses business goals that can be achieved using the software. It also includes information on system sizing, checklists, and best practices.

- The *Opware® SAS 5.2 Configuration Guide* is intended to be used by system administrators who are responsible for all facets of configuring the Opware Command Center. It documents how to set up users and groups, configure Opware server management, and setting up the main Opware Command Center features, such as patch management, configuration tracking, software repository replicator setup, code deployment, as well as OS and software provisioning.

Contacting Opware, Inc.

The main web site and phone number for Opware, Inc. are as follows:

- <http://www.opware.com/index.htm>
- +1 (408) 744-7300

For links to the latest product documentation and software downloads, see the Opware Customer Support site:

- <https://download.opware.com/opsw/main.htm>

For troubleshooting information, you can search the Opware Knowledge Base at:

- <https://download.opware.com/kb/kbindex.jspa>

The Opware Customer Support email address and phone number follow:

- support@opware.com/
- +1 (877) 677-9273

Chapter 1: Installing and Configuring the DCI Report Server

IN THIS CHAPTER

This chapter discusses the following topics:

- Prerequisites
- Installing the DCI Report Server
- Configuring DCI Report Servers in a Multimaster Mesh

The DCI Report Server 1.6 is a software package on the DCI Report Server disk of the Opware Server Automation System (SAS) Installation DVDs. The DCI Report Server must be installed using the Intelligent Software Module (ISM) Tool.

Before you install the DCI Report Server, Microsoft Internet Information Services (IIS) must be installed and running on your managed server. The installation process creates a virtual directory, DCI (the alias for this web site), under the IIS web site default directory that points to a real directory on the server. The path of the directory where the content will reside is %SystemDrive%\Program Files\Opware\DCI\wwwroot.

Prerequisites

To install the DCI Report Server, you need the following hardware, server setup, and user privileges.

Hardware

You need the following items to begin installing the DCI Report Server:

- A Pentium III CPU or higher (Pentium 4 at 2 GHz or more recommended)
- 256 MB RAM or higher (512 MB recommended, more for heavy usage)
- 800 MB of free disk space to download and install the DCI package. Installed software is approximately 320 MB

- An Opware managed server (a server with an Opware Agent that is managed through the Opware Command Center)
- On Windows 2000, Service Pack 4 or higher, running the Internet Information Services 5.0 or 6.0
- On Windows 2003, Internet Information Services 6.0
- If you plan to run the DCI server with an Opware Network Automation System (NAS) server, the Opware NAS server must be running with an Oracle database. Consult your Opware NAS system administrator for more information.

Software

DCI Report Server 1.6 is only compatible with Opware SAS 5.2 and Opware NAS 4.0.

Preparing the Server

To install the DCI Report Server, your server must meet the following conditions:

- The machine is available to Opware users and the named machine is accessible in the Opware Command Center from the Servers ► Manage Servers page.
- IIS is installed on your machine. To verify this, the following programs should be present on the computer:
 - Programs ► Administrative Tools ► Internet Services Manager
 - Or
 - Programs ► Administrative Tools ► Services ► IIS Admin Service
 - Or
 - Programs ► Administrative Tools ► Internet Information Services (IIS) Manager
- The DCI Report Server DVD-ROM is loaded on your computer.
- The DCI server can resolve the hostname “truth” to the desired Opware database server.
- The database can accept connections on default port 1521.
- The following information is related to your Opware SAS configuration. These values will be required to configure custom attributes for the DCI Report Server once it has

been installed. All NAS information is optional and only required if you plan to use DCI with a NAS server.

- DCI administrator's user name: _____
 - DCI administrator's password: _____
(This password needs to meet security requirements on the DCI Server.)
 - Hostname or IP address of the NAS server (optional): _____
 - Port number for the NAS server (optional): _____
 - Password for the NAS Oracle database (optional): _____
 - SID for the NAS Oracle database (optional): _____
(Make sure that you use the database SID, not the database service name.)
 - User name for the NAS Oracle database (optional): _____
 - IP address of the OCC Server: _____
 - Opware_public_views password: _____
 - SID for the Model Repository database: _____
(Make sure that you use the database SID, not the database service name.)
- Before you install the DCI Report Server, perform the following steps:
 - If you plan to run the DCI Report Server with a NAS server, you need the Oracle SID for your NAS server. (DCI is only compatible with NAS servers that use an Oracle database.)
 - Check and make a note of the operating system running on this server.
 - If you are upgrading from the a previous version of the DCI Report Server, you must completely uninstall the DCI Report Server and then follow all the steps in this chapter. See Chapter 3, "Uninstalling, Moving, or Upgrading DCI Report Server" for more information.



The DCI Report Server installation file is about 320 megabytes and can take a while to upload, depending on your network connection. You must have the appropriate permissions to manage software packages in the Opware Command Center to perform this upload.

Getting Proper User Privileges

Before you can begin installing and configuring DCI, ensure that you are an administrator user that belongs to the Advanced Users group in the Opware Command Center.

If the Advanced Users group is customized and has lost some of the necessary permissions required for installing and configuring DCI, ensure that the user performing the installation and configuration of DCI belongs to a group that has the following permissions:

- Wizard: Install Software
- Wizard: Uninstall Software
- Data Center Intelligence Reports
- Read permissions on the Other Applications and System Utilities stacks.
- Write permission to the facility and customer of the server

To add a user to Administrator and Advanced User groups, perform the following steps:

- 1** Log in to the Opware Command Center as an administrator user.
- 2** From the navigation panel, click Administration ► Users & Groups. The Manage Users: View Users page appears. By default, the Users tab page displays.
- 3** Click the Administrators tab. The View Administrators page shows current Opware administrators.
- 4** Click the **New Administrator** button. The Users & Groups: Add Administrators page appears.
- 5** Select a user from the list.
- 6** Click the **Save** button. The Opware Command Center displays a confirmation message.
- 7** Click the **Continue** button.
- 8** The Opware Command Center adds the user to the current list of Opware administrators and displays an updated Users & Groups: View Administrators page.
- 9** To add this user to the Advanced Users group, on the Users & Groups: View Administrators page, click the Groups tab. The Users & Groups: View Groups page appears showing a list of all groups.

- 10** Click the Advanced Users link name. The Users & Groups: Edit Group - Advanced Users page appears with the User tab selected showing a list of users that you can choose from.
- 11** In the Unassigned Members box, highlight the names of the members you want to add to the Advanced Users group, and click the left-pointing arrow to move the names into the Assigned Members box.
- 12** When you finish selecting members, click **Save**. A confirmation page appears.
- 13** Click **Continue** to return to the Assign Users page. The user now has the proper user privileges to install and configure DCI.

Installing the DCI Report Server

To install the DCI Report Server, you need the Opware ISMTool version shipped with the DCI Report Server 1.6 release. You will also need an Opware SAS login and password to download the ISMTool. Contact support@opware.com if you do not already have a login and password.

To install the DCI Report Server using the ISMTool, perform the following steps:

- Uninstall the Older Version of ISMTool
- Install the ISMTool
- Unpack and Upload the DCI Report Server Package
- Set Custom Attributes Values on DCI Report Server Software Node
- Install the DCI Report Server Software

Uninstall the Older Version of ISMTool

DCI Report Server 1.6 will only work with ISMTool version shipped with the release. So, if you have a previous version of the ISMTool installed, you will need to uninstall it.

To uninstall the older version of the ISMTool, perform the following steps:

- 1** Log on to the computer where the older version of the ISMTool is installed.
- 2** From the Control Panel ► Add Remove Programs, locate the ISMTool application and remove the older version of the ISMTool application.
- 3** Log off and then back on to the computer, and then install the newer version of the ISMTool.

Install the ISMTool

To install the ISMTool on any Windows 2000 or 2003 managed server, perform the following steps:

- 1** From the Opware Command Center, go to the Servers ► Manage Servers page.
- 2** Find the Windows server to install the DCI Report Server software on, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 3** Check the box for the server, and from the **Software** menu choose **Tasks ► Install ► Application**. The Install Software Wizard window launches.
- 4** In the Select software page, navigate to System Utilities ► Opware Tools ► ISMTool.
- 5** You will see a list of operating systems that the ISMTool supports. Scroll down to either Windows 2000 or 2003 and check the box next to it to select the ISMTool for installation.
- 6** Click **Next**.
- 7** In the Confirm Selection page, double-check all the parameters of your selections, and then click **Preview**.
- 8** After the preview has finished, click **Next**.
- 9** In the Schedule and Notify page, you have the option of scheduling the ISMTool installation, or installing it immediately:
 - If you want to install immediately, click **Install**.
 - If you would like to schedule the installation, in the Schedule section, choose Run Now. In the Notify section, choose if you want to send an e-mail when the installation has finished. When you have finished setting a scheduled time for installation, click **Schedule**.
- 10** When the installation has finished, you can click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page after it has installed.
- 11** Click **Close** to exit the installation.

Unpack and Upload the DCI Report Server Package

To unpack and upload the DCI Report Server software package, perform the following steps:

1 Copy the `DCIPackage_en-1.6.ism` package to an accessible location on the computer where the ISMTool is installed.

2 Open a command prompt and go to the directory where the ISM has been copied to.

3 Execute the following command:

```
ismtool --unpack DCIPackage_en-1.6.ism
```

4 Next, execute the following command:

```
ismtool --upload DCIPackage_en-1.6
```

5 You will be prompted to respond to the following confirmation

```
Using an agent gateway to reach an Opware Core
```

```
Is this correct? [y/n]:
```

6 Type `y` for yes and press ENTER.

7 At the Opware user name and login prompt, enter the Opware Administrator user name and password.

8 At the Opware customer prompt, enter:

```
Customer Independent
```

After successfully uploading, you will see a message stating "Update complete."

Set Custom Attributes Values on DCI Report Server Software Node



The following steps are critical for the report server to correctly connect to the database. If an attempt to access a report from the Report home page fails after installation, review this information.

To set custom attributes to the DCI Report Server software node, perform the following steps:

- 1** From the Opware Command Center, from the Software link in the navigation bar, click Applications ► Other Applications, then navigate to the DCI ► en ► 1.6 ► Windows 200<?> ► DCI 1.6.
- 2** Select the Custom Attributes tab.
- 3** Click **Edit**.
- 4** In the Custom Attributes page DCI server, enter the custom attribute values. These attributes are required, and the installation will fail if any of them are missing or incorrect.

Table 1-1: DCI Software Node Custom Attribute Configuration – Required Attributes

CUSTOM ATTRIBUTE	DESCRIPTION
dci_admin_user	The user name for the admin user to be created on the DCI server.
dci_admin_pwd	The password for the DCI admin user. By default, this password is <code>Opware0</code> , but this can be changed.
occ_ip	The IP address of the Opware Command Center (OCC) to be configured for reporting access.
public_views_pwd	The password for the Opware_public_views user.
sas_db_sid	The SID of the Opware Data Repository database. (Make sure that you use the database SID, not the database service name.)

Figure 1-1 illustrates the DCI software node custom attribute fields.

Figure 1-1: DCI Software Node Custom Attribute Fields

Applications > Other Applications > DCI > en > 1.5 > Windows 2000 > dci-1.5

dci-1.5

Properties Packages 3 Custom Attributes 10 Install Order 0 Members 1 Config Tracking Templates 0 History

The following custom attributes are for this Node **Add Custom Attributes**

Name	Inherited Value	Local Value
dci_admin_pwd		Opware0 <input type="checkbox"/> Delete
dci_admin_user		dciadmin <input type="checkbox"/> Delete
nas_db_host		192.168.160.39 <input type="checkbox"/> Delete
nas_db_port		1521 <input type="checkbox"/> Delete
nas_db_pwd		oracle <input type="checkbox"/> Delete
nas_db_sid		m039 <input type="checkbox"/> Delete
nas_db_user		SYSTEM <input type="checkbox"/> Delete
occ_ip		192.168.165.98 <input type="checkbox"/> Delete
public_views_pwd		opsware_admin <input type="checkbox"/> Delete
sas_db_sid		truth <input type="checkbox"/> Delete

Save Cancel

- 5** If you plan to run the DCI server with a NAS server, then you will also need to enter values for the following attributes. These additional attributes are only needed to enable reporting from the Opware Network Automation System. They must either all be blank, or all have appropriate values.

Table 1-2: DCI Software Node Custom Attribute Configuration – NAS Server Option

CUSTOM ATTRIBUTE	DESCRIPTION
nas_db_host	The hostname or IP address of the NAS database.
nas_db_port	The port on which the NAS database accepts connections.
nas_db_sid	The SID of the NAS database. (Make sure that you use the database SID, not the database service name.)
nas_db_user	The user name of the NAS database.

Table 1-2: DCI Software Node Custom Attribute Configuration – NAS Server Option

CUSTOM ATTRIBUTE	DESCRIPTION
nas_db_pwd	The password for the NAS database.



You can run the DCI server with the OCC alone, with the OCC and NAS, but not with NAS alone. If you do plan to run DCI Report Server with a NAS server, then you will need to fill out all NAS attributes.

6 Click **Save**.

Install the DCI Report Server Software

To install the DCI Report Server software, perform the following steps:

- 1** Find the server intended to host the DCI Report Server, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2** Check the box for the server, and from the **Software** menu choose **Tasks ► Install ► Application**. The Install Software Wizard window launches.
- 3** Click Other Applications, then navigate to the DCI ► en ► 1.6 ► Windows 200<?>.
- 4** Select the check box in front of dci-1.6 and click **Next**.
- 5** In the Confirm Selection page, double-check all the parameters of your selections, and then click **Preview**.
- 6** After the preview has finished, click **Next**.
- 7** In the Schedule and Notify page, you have the option of scheduling the ISMTool installation, or installing it immediately:
 - If you want to install immediately, click **Install**.
 - If you would like to schedule the installation, in the Schedule section, choose Specify Time and select a time from the drop-down list. If you want to send e-mail when the installation has finished, in the Notify section, choose Condition and enter the e-mail addresses. When you have finished setting a scheduled time for installation, click **Schedule**.

- 8** When the installation has finished, click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page.
- 9** Click **Close** to exit the installation. You are now ready to enable the Opsware Command Center so that other Opsware users can access the report server.
- 10** Next, from the navigation bar click the Configuration link to go to the System Configuration page.
- 11** On this page, click the Opsware Command Center link.
- 12** Scroll down the page and double-check the parameter named `owm.features.Reports.allow`. Ensure that the value is set to `true`. True means that the installation was successful. If the value is set to `false`, there was a problem with the installation and you will need to troubleshoot the error. If you see a true value, click **Save** at the bottom of the page. You should now see the Reports link in the navigation panel.

Configuring DCI Report Servers in a Multimaster Mesh

In a very basic deployment, a single core would run a single DCI Report Server. Depending upon your environment, however, you could be running a multimaster mesh (multiple cores) with several cores pointing at a single DCI Report Server.

As your mesh becomes more complex, you might want to add more DCI servers to your multimaster mesh. For example, your multimaster mesh might have one DCI Report Server designated to run reports for a certain group of cores, and a second DCI Report Server designated for a different set of cores.

In these situations, you will need to make modifications to custom attributes on the DCI Report Server and use the DCI reconfigure control to configure the mesh properly.

Remember that when you first installed the DCI Report Server software node, the custom attribute `occ_ip` was set at the node level to point to the core that you installed the DCI Report Server on. In order to enable additional cores in the mesh to be able to view reports from a single DCI Report Server, you need to add or modify the `occ_ip` custom attribute on the DCI Report Server itself. When you set a custom attribute at the server level, that value will override that attribute for any nodes attached to that server (in this case, the DCI Server software node).



This section applies to multiple DCI Report Servers that are running on the same operating system – Windows 2000 or Windows 2003. If you introduce a new DCI Report Server that runs on a different operating system than the DCI Report Server already installed in your core, then you need to set the proper custom attributes on the DCI software node following the instructions found at “Set Custom Attributes Values on DCI Report Server Software Node” on page 8. Then, install the new DCI Report Server following the regular DCI Report Server instructions, found at “Install the DCI Report Server Software” on page 10.

The following section shows you how to configure the following two DCI Report Server configuration scenarios:

- Configuring a Single DCI Server in a Multimaster Mesh
- Configuring Multiple DCI Servers in a Multimaster Mesh

Configuring a Single DCI Server in a Multimaster Mesh

If you are using a single DCI Report Server in a multimaster mesh and would like to have more than one core to view reports from that DCI Report Server, you need to add or change the custom attribute named `occ_ip` on the DCI Report Server so that it points to another core in the multimaster mesh. The DCI reconfigure control enables you to set this attribute on the DCI Report Server.

To configure additional cores in a multimaster mesh to view a DCI Report Server, perform the following steps:

- 1** Find the server that hosts the DCI Report Server, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2** Click the server name link.
- 3** On the server property page, select the Custom Attributes tab.
- 4** Click the **Edit** button.
- 5** Edit the value of the custom attribute named `occ_ip` and enter the IP of the new core you would like to point to the DCI Report Server.
- 6** Click **Save**.
- 7** Find the DCI Report Server again, by name or IP address from Servers ► Manage Servers, or by Server Search.

- 8** Select the check mark next to the server.
- 9** From the **Tasks** menu, choose **Run ► Control**.
- 10** In the DCI Control dialog box, from the Application drop down list, make sure you choose dci-1.6 (Server) and that the Action drop down list is set to Reconfigure.
- 11** Click **Run**.
- 12** After the reconfigure control has finished running, from the navigation bar click the Configuration link to go to the System Configuration page.
- 13** On this page, click the Opware Command Center link.
- 14** Click **Save** at the bottom of the page. Even if you make no changes, click **Save** to ensure the proper configuration.



When you run the DCI reconfigure control, the Apache server will be restarted and any users logged into the OCC at the time will be logged off.

Configuring Multiple DCI Servers in a Multimaster Mesh

If you would like to run more than one DCI Report Server in a multimaster mesh, you will need to install each additional DCI Report Server and reconfigure the custom attribute `occ_ip` for that server to point to specific cores in the mesh.

To introduce a second DCI Report Server into the mesh, you first need to add a new custom attribute named `occ_ip` on the new DCI Report Server, set the `occ_ip` attribute value to the IP address of a new core, and then install the new DCI Report Server software node on the new server.

The reason that you need to create and set a new `occ_ip` custom attribute value on the second DCI Report Server is that you cannot have two DCI Report Servers pointing to the same core. Thus for the second DCI Report Server, you will override the `occ_ip` value that was originally set on the DCI Report Server software node. Remember that when you set a custom attribute at the server level, that value will override the same attribute for any nodes attached to that server (in this case, the DCI Report Server software node).

To configure multiple DCI Servers in a multimaster mesh, perform the following tasks:

- Install the DCI Report Server Software with New Custom Attribute
- Run the DCI Reconfigure Control

Install the DCI Report Server Software with New Custom Attribute

To install a new DCI Report Server in a multimaster mesh, perform the following steps:

- 1** Find the server intended to host the DCI Report Server, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2** Select the server link (the server's name).
- 3** In the server's property page, select the Custom Attributes tab.
- 4** In the Custom Attributes page for the server, click **New**. New attribute fields appear at the bottom of the attribute list.
- 5** From the Name column, enter
`occ_ip`
as the new attribute name.
- 6** In the Value column, enter the IP address of the core you want to point to the new DCI Report Server.
- 7** Click **Save**.
- 8** Click the Return to Manage Servers link.
- 9** To find the DCI Report Server you just added the new custom attribute to, search by name or IP address from Servers ► Manage Servers, or by Server Search.
- 10** Check the box for the server, and from the **Software** menu choose **Tasks ► Install ► Application**. The Install Software Wizard window launches.
- 11** Click Other Applications, then navigate to the DCI ► en ► 1.6 ► Windows 200<?>.
- 12** Select the check box in front of dci-1.6 and click **Next**.
- 13** In the Confirm Selection page, double-check all the parameters of your selections, and then click **Preview**.
- 14** After the preview has finished, click **Next**.
- 15** In the Schedule and Notify page, you have the option of scheduling the ISMTool installation, or installing it immediately:
 - If you want to install immediately, click **Install**.
 - If you would like to schedule the installation, in the Schedule section, choose Specify Time and select a time from the drop-down list. If you want to send e-mail when the installation has finished, in the Notify section, choose Condition and

enter e-mail addresses. When you have finished setting a scheduled time for installation, click **Schedule**.

- 16** When the installation has finished, you can click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page.
- 17** From the navigation bar, click the Configuration link to go to the System Configuration page.
- 18** On this page, click the Opsware Command Center link.
- 19** Scroll down the page and double check the parameter named `owm.features.Reports.allow`. Make sure the value is set to true. True means the installation was successful. If the value is set to false, there was a problem with the installation and you will need to troubleshoot the error. If you see a true value, click **Save** at the bottom of the page.
- 20** You should now see the Reports link in the navigation panel.

Run the DCI Reconfigure Control

Once you have installed a second DCI Report Server in your multimaster mesh, use the DCI reconfigure control to configure a core to point to the DCI Report Server.



This task is only necessary if additional cores need to be configured.

To run the DCI reconfigure control, perform the following steps:

- 1** Find the server that hosts the DCI Report Server, by name or IP address from Servers **►** Manage Servers, or by Server Search.
- 2** Select the check box next to the server (do not click the server name link).
- 3** From the **Tasks** menu, choose **Run ► Control**.
- 4** In the DCI Control dialog box, from the Application drop down list, make sure you choose `dci-1.6 (Server)` and that the Action drop down list is set to Reconfigure.
- 5** Click **Run**.



When you run the DCI reconfigure control, the Apache server will be restarted and any users logged into the OCC at the time will be logged off.

- 6** After the reconfigure control has run, from the navigation bar, click the Configuration link to go to the System Configuration page.
- 7** On this page, click the Opware Command Center link.
- 8** Scroll down the page and click **Save**. Even if you make no changes, click **Save** to ensure the proper configuration.
- 9** You should now see the Reports link in the navigation panel.

Chapter 2: Uninstalling, Moving, Upgrading DCI

IN THIS CHAPTER

This chapter contains the following topics:

- About Uninstalling, Moving, Upgrading DCI Report Server
- Uninstalling the DCI Report Server
- Moving DCI Report Server
- Upgrading the DCI Report Server

About Uninstalling, Moving, Upgrading DCI Report Server

This chapter shows you how to uninstall, move, and upgrade the DCI Report Server. These instructions assume that you are working with a single DCI Report Server in a core. Special considerations regarding multiple DCI Report Servers in a multimaster mesh are discussed where relevant.

Uninstalling the DCI Report Server

To uninstall the DCI Report Server, perform the following steps:

- 1** Find the server you want to uninstall the DCI Report Server from, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2** Check the box for the server, and from the **Software** menu choose **Tasks** ► **Uninstall** ► **Application**. The Uninstall Software Wizard window launches.
- 3** Select the DCI application and click **Next**.
- 4** In the Confirm selections page, verify that you have selected the correct software (DCI) and the correct server, and then click **Preview**.

- 5** Wait for the Preview to complete, and then from the **View Details** button, verify the status is Completed and the Output tab shows that the DCI software node will be uninstalled. Click **Close**.
- 6** Click **Next**.
- 7** In the Schedule and Notify page, you have the option of scheduling the DCI uninstallation, or uninstalling it immediately:
 - If you want to install immediately, click **Uninstall**.
 - If you would like to schedule the installation, in the Schedule section, choose Specify Time and select a time from the drop-down list. If you want to send e-mail when the installation has finished, in the Notify section, choose Condition and enter e-mail addresses. When you have finished setting a scheduled time for installation, click **Schedule**.
- 8** When the installation has finished, you can click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page.
- 9** Once the uninstall software wizard completes, from the navigation bar click the Configuration link to go to the System Configuration page.
- 10** On this page, click the Opsware Command Center link.
- 11** Scroll down the page and double check the parameter named `owm.features.Reports.allow`. Ensure that the value is set to `false`. False means the uninstallation was successful. If the value is set to `true`, there was a problem with the installation and you will need to troubleshoot the error. If you see a false value, click **Save** at the bottom of the page – even if you do not make any changes to the page. The Reports link in the navigation panel will be removed.



On the server where DCI was installed, make sure that the DCI virtual directory on IIS (DCI under default web site) has been fully removed and that the `\Program Files\Opsware\DCI\wwwroot` directory is absent or contains only a logs directory.

Moving DCI Report Server

In order to move the DCI Report Server, you need to first uninstall the DCI Report Server then reinstall it in its new location. For information on how to uninstall and install, see the following tasks:

- Uninstalling the DCI Report Server on page 17
- Installing the DCI Report Server on page 5

Updating DCI Report Server in Multimaster Mesh

If the DCI Report Server being moved to a multimaster mesh (with multiple OCCs), see the Configuring DCI Report Servers in a Multimaster Mesh on page 11 or more information.

Upgrading the DCI Report Server

In order to upgrade the DCI Report Server, you need to first uninstall the DCI Report Server then reinstall the new version. For information on how to uninstall and install, see the following tasks:

- Uninstalling the DCI Report Server on page 17
- Installing the DCI Report Server on page 5

When you upgrade the DCI Report Server, any existing custom reports will be backed up during uninstallation, so you will not need to reinstall them. After the new version of DCI is installed, the custom reports will be restored to the appropriate structure (prior to the uninstallation).

Chapter 3: DCI Reports

IN THIS CHAPTER

This section covers the following topics:

- About DCI Reporting
- Accessing DCI Reports in the OCC
- Report Parameters
- Report Results
- DCI Reports

About DCI Reporting

Welcome to Opsware's DCI Reporting. DCI reports provide real-time comprehensive information about your organization's servers, compliance, software, customers, operating systems, patches, compliance policies and what changes have occurred and should occur. After an action completes in the Opsware Command Center (OCC), it is available in the DCI reports.

This help provides an overview of how to use the DCI Report Server, introduces DCI concepts, and explains the various reports so you can be effective using Opsware's DCI Reports.

Accessing DCI Reports in the OCC

The home page is divided into five main sections: Server Reports, Network Reports, Compliance Center, Custom Reports, and Ad Hoc Reporting.



Network reporting requires the purchase of the Opware Network Automation System (NAS) product. If you have not purchased the NAS product, you will not see the Network Reports link in the OCC.

Figure 3-1: The DCI Home Page – Server Reports Page

The screenshot shows the DCI Home Page interface. At the top, there is a navigation bar with a search field and a 'Go' button. Below the navigation bar is a sidebar menu with the following items: Home, My Jobs, Servers, Software, Environment, and Reports. The 'Reports' item is highlighted with a red box. The main content area is titled 'Home' and contains a 'Tasks' section. The 'Tasks' section is a table with four columns: OS Provisioning, Patch Management, Software Provisioning, and Power Tools. The 'View Reports' link in the Power Tools column is circled in red.

OS Provisioning	Patch Management	Software Provisioning	Power Tools
Install OS	Install Patch	Install Software	Launch OCC Client
Prepare OS	Uninstall Patch	Uninstall Software	Run Distributed Script
	Upload Patch	Install Template	Run Custom Extensions
	Microsoft Patch Update	Deploy Code	View Reports

If you click a Reports link from the Navigation bar, the screen displays a page of available reports for each reporting category. From each report page, clicking on the name of any report folder will generate a list of associated reports in the lower pane of the DCI window. For example, clicking on Change History under the Server Reports link will display the following page shown in Figure 3-2.

Figure 3-2: Server Reports Page - Change History Reports

The screenshot shows the Opware Command Center interface. At the top, the user is identified as Patrick Holan with options for 'My profile' and 'Log Out'. The time is 23:04 UTC. The navigation bar includes a search function for servers. The left sidebar contains a navigation menu with categories like Home, My Jobs, Servers, Software, Environment, Reports, and Administration. The main content area is titled 'Reports / Server Reports / Change History' and is divided into two sections. The 'Server Reports' section shows a tree view of folders: Change History, Software and Patch Policies, Users and Security, Servers, Facilities, and Customers, and Software and Patch State. The 'Reports' section lists several reports with their descriptions:

- Configuration Backups by Server**: Monitored configuration backup events for one or more servers
- Configuration Backups by Server Group**: Monitored configuration backup events for one or more server groups
- Recent Jobs by Date**: Recent jobs organized by date and time
- Recent Jobs by Server**: Recent jobs for one or more servers
- Recent Jobs by User**: Recent jobs for one or more users
- Recent Patch Jobs**: Recent patching on one or more servers, organized by operating system

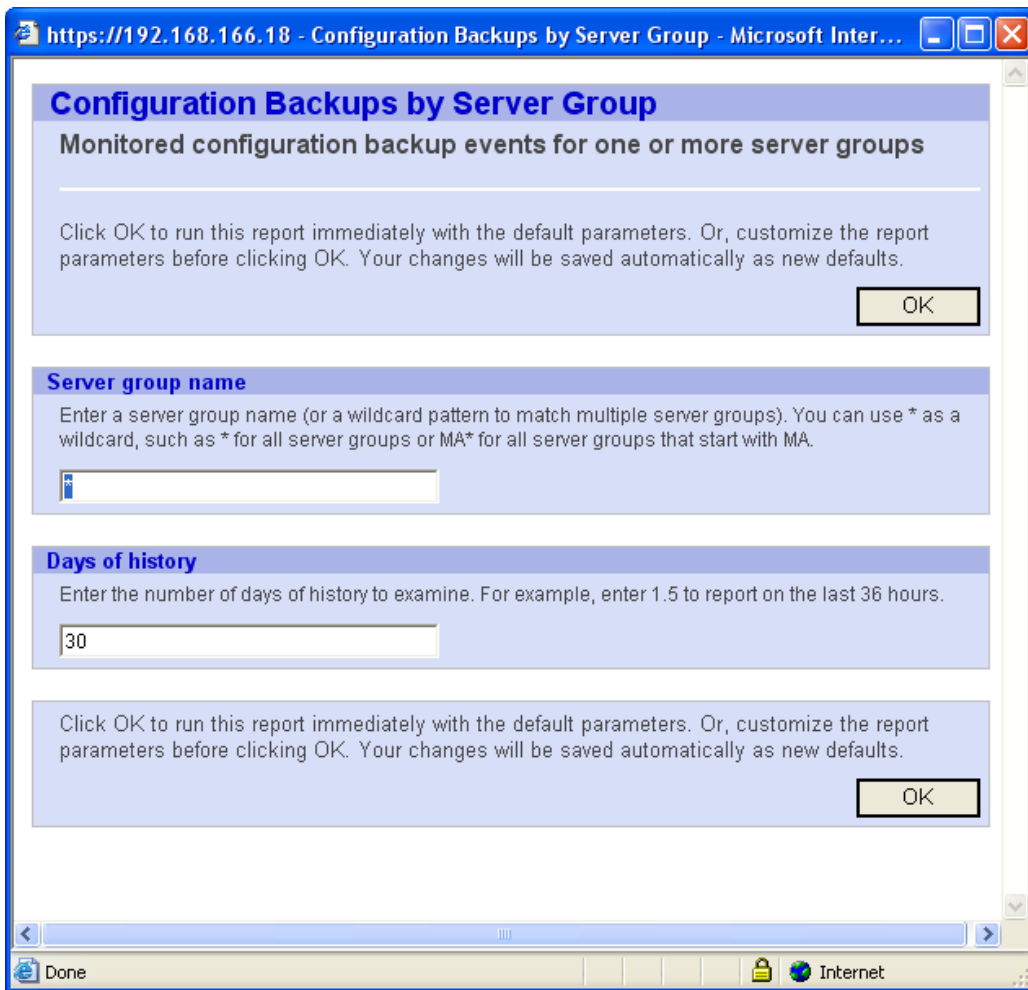
Clicking on the name of a report will launch either the report itself or a new window to set the parameters for the report.

Report Parameters

Many reports require input parameters in order to be run. For reports that require parameters, you can run the report with its default parameter values or modify the parameter values. To run a report using its default parameters, simply click the OK button at the top or bottom of the screen (or press ENTER).

If you would like to customize a report's criteria, enter your own custom values in the report chooser window and then click the OK button. In many cases reports parameters include a server or server group name and a days of history field to indicate a time frame, as shown in Figure 3-3. Once you customize a report's parameter values these values are saved as the new default parameters for your user account.

Figure 3-3: Sample Chooser Screen



The screenshot shows a web browser window with the title "https://192.168.166.18 - Configuration Backups by Server Group - Microsoft Inter...". The main content area has a blue header with the text "Configuration Backups by Server Group" and "Monitored configuration backup events for one or more server groups". Below the header, there is a paragraph of text: "Click OK to run this report immediately with the default parameters. Or, customize the report parameters before clicking OK. Your changes will be saved automatically as new defaults." followed by an "OK" button. The next section is titled "Server group name" and contains the instruction: "Enter a server group name (or a wildcard pattern to match multiple server groups). You can use * as a wildcard, such as * for all server groups or MA* for all server groups that start with MA." Below this is a text input field containing "*". The following section is titled "Days of history" and contains the instruction: "Enter the number of days of history to examine. For example, enter 1.5 to report on the last 36 hours." Below this is a text input field containing "30". At the bottom of the form area, there is another paragraph of text: "Click OK to run this report immediately with the default parameters. Or, customize the report parameters before clicking OK. Your changes will be saved automatically as new defaults." followed by an "OK" button. The browser's status bar at the bottom shows "Done" and "Internet".

To set custom report parameters, enter the following information:

- **Server/Server Group Name:** Use the full name for servers (not IP addresses) and server groups or use a name plus an asterisk ("*") to search by name. For example: "Develop*".

- **Days of History:** Enter the number of days of history to examine. For example, enter 2 to report on the last 48 hours.

Not all reports will require entering parameters, and some reports will require only a single parameter, such as server name, days of history, or future days.

Report Results

Report results initially appear in a graphical or list view. The graphical view provides a quick overview of the available data for this report in a chart. Clicking on any of the bars in the chart will drill down to more detail on the selected item only. You can drill down to individual servers that appear in a report and get detailed information about a server.

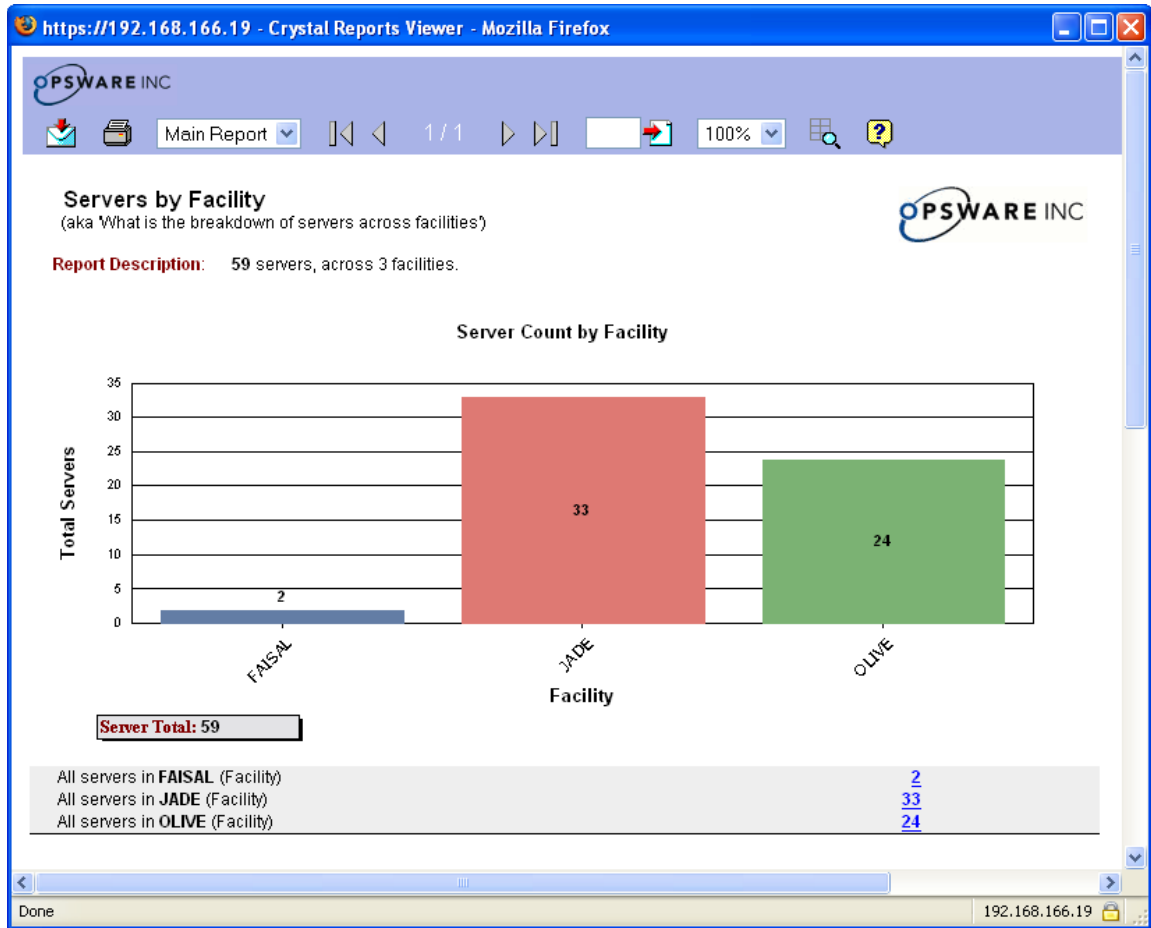
This section discusses the types of DCI report results and contains the following topics:

- Graphical View Report Results
- List View Report Results
- Individual Server Results View
- Report Results Toolbar Buttons

Graphical View Report Results

Figure 3-4 shows the server report named “All Servers By Facility” in a graphical view.

Figure 3-4: Graphical View of Report All Servers By Facility



Many of the elements inside the report are clickable, enabling you to drill down and display more detailed information about specific information on the results. Each time you go to a different page of the report, you can right-click and choose Back to navigate to pages you already visited. See “Report Results Toolbar Buttons” on page 29 in this chapter for more information on more accurate report results navigation.

For example, if you click the center bar for the Jade facility, a more detailed view of the servers in this facility is displayed, as shown in Figure 3-5.

Figure 3-5: Servers By Facility – Detailed View



This more detailed view lists all servers in this facility distinguished by operating system (OS). You can keep drilling down to individual servers by clicking any live links.

List View Report Results

Some reports appear in a table format with an expandable tree view on the left called the Group Tree. The group Tree view allows you to easily navigate levels of your report. Clicking the links in a report will drill down to the specific data for the link you selected.

Many reports have multiple levels of information to fine tune your reporting results. This type of report result is illustrated in Figure 3-6 for the report Recent Jobs by Date. This report shows all recent jobs run in the core (Jade), and if you expand the left side of the report you see each type of job arranged by the server operating system the job was run on.

Figure 3-6: List View Report Result for Recent Jobs by Date Report

Recent Jobs by Date

Report Description: Results for all jobs over the past 30 days: 145 unique jobs resulting in 208 servers and 3 unique users.

	# Unique Jobs	# Server Actions
jade (Facility)	145	208
Red Hat Enterprise Linux AS 3	37	46
Audit Configuration	18	18
Audit Servers	3	4
Communication Test	5	11
Create Snapshot	2	2
Install Template	1	1
Push Configuration	5	5
Reconcile	1	1
Run Script	2	4
Red Hat Linux 7.2	20	20
Audit Configuration	9	9
Audit Servers	1	1
Communication Test	4	4
Create Snapshot	1	1
Push Configuration	2	2

Individual Server Results View

Drilling down to a specific server will result in a tabbed window showing detailed reporting information for that computer, as shown in Figure 3-7.

Figure 3-7: Detailed View of Individual Server

The screenshot shows a web browser window displaying the Crystal Reports Viewer. The address bar shows the URL `https://192.168.163.147 - Crystal Reports Viewer - Mozilla Firefox`. The page header features the Opsware Inc logo and a toolbar with icons for navigation and search. The main content area displays the report title `m022.qa.opsware.com (192.168.160.22)` and a set of tabs: `Properties`, `Property Change Log`, `Software & Patches`, `Unreconciled Software`, and `Job History`. The `Properties` tab is selected, showing two sections: `Management Information` and `Reported Information (as of 5/24/2005 6:41:56PM UTC)`.

Management Information	
Name	m022.qa.opsware.com
Notes	(Joe) Used for DCI and ISM testing.
IP Address	192.168.160.22
OS Version	SuSE Linux Enterprise Server 8
Customer	joe-cust
Facility	TOMATO
Server Use	Joe-Use
Deployment Stage	Joe-Stage
Opsware Lifecycle	Managed
Agent Status	OK

Reported Information (as of 5/24/2005 6:41:56PM UTC)		
Agent Version	30.0.2.102	
Hostname	m022.qa.opsware.com	
Reported OS	Linux SLES-8	
Serial Number	6J0CFCX2J0R3	
Chassis ID	6J0CFCX2J0R3	
Manufacturer	COMPAQ	
Model	PROLIANT DL360	
CPUs (1)	Speed	Cache Size
	797	256
Memory	Type	Capacity
	Swap	1.00 GB
	RAM	1,008.93 MB

Each server details window shows a server's properties, properties change log, software packages, unreconciled software, and job history. Click on any one of the tabs to view detailed server property information.

Report Results Toolbar Buttons

Each generated report has a toolbar with a set of buttons at the top. These buttons can be used to click through the pages of the report, search for a particular page, print the report, export the report in various formats, and get help. Reports can be exported in Excel, Word,

Acrobat, Crystal Reports and rich text format. Reports do not tally the number of pages in advance. Therefore, 1-1+ will display initially, with this display changing as you click through the pages of a report. Table 3-8 illustrates the report results icons.

Figure 3-8: Report Results Toolbar Buttons



Table 3-3 describes the DCI report toolbar buttons.

Table 3-3: DCI Report Toolbar Buttons






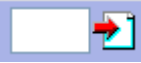
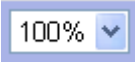

BUTTON	DESCRIPTION
	<p>Group Tree</p> <p>A tree list that displays values on which the report is grouped. For example, if you generate a report that groups by servers, you will see a list of servers.</p> <p>For example, if you are generating a report that searches for servers, this tree will display a list of servers that you can select to access specific information about each server returned in the report results. For other reports, this list might display server groups, patches, jobs (listed by operating system), configuration backups, and so on.</p> <p>Clicking this icon will hide or show the list.</p>
	<p>Export</p> <p>Click this button to export the report results. Reports can be exported in Excel, Word, Acrobat, Crystal Reports and rich text format.</p>
	<p>Print</p> <p>Click this button to print the report. A PDF of your report appears. From the Adobe Acrobat reader in your browser, select print.</p>

Table 3-3: DCI Report Toolbar Buttons

BUTTON	DESCRIPTION
	<p>Main Report Toggle</p> <p>This drop down list allows you to toggle between levels of your report from various search results.</p>
	<p>Page Scroll</p> <p>Use the arrow keys to scroll from page to page in your report results (for reports more than one page long). The left most arrow takes you to the first page of the report results, while the right most arrow takes you to the last page of the report results. The left and right arrow buttons in the center enable you scroll one page at a time.</p>
	<p>Page Jumper</p> <p>Enter the number of the page you want to jump to and then click the red arrow on a page icon.</p>
	<p>Zoom</p> <p>Allows you to zoom in or out of the report results.</p>
	<p>Advanced Search</p> <p>Click this icon to access advanced search features.</p>

DCI Reports

DCI Reports are available to users who have been granted the appropriate permissions. Five reporting types are available from the OCC navigation panel. Each area links to a set of related reports organized into folders. Some of these reports are repeated in different areas to provide complete sets of compliance standards reports.

DCI provides the following categories of reports:

- **Server Reports:** Reports about Opsware Server Automation System (SAS), such as server changes, server facilities and customers, software and patches, and users and security.

- **Network Reports:** If the Opware Network Automation System (NAS) is installed and DCI is configured for NAS, reports about the network environment, status, and health will display here.
- **Compliance Center:** Reports for compliance standards including COBIT, COSO, ITIL and Sarbanes Oxley.
- **Custom Reports:** Specific reports created for particular needs in your operational environment.
- **Ad-hoc Reports:** Configurable report interface to create reports about specific software, servers, patches and the Opware model, grouped and filtered according to your needs.

Server Reports

The following Opware Server Automation System (SAS) pre-built reports are available in the Server Reports section in the OCC navigation bar:

- Change History Reports
- Software and Patch Policies
- Software and Patch State
- Servers, Facilities, and Customers
- Software and Patch State

Note that all reports involving Server Groups will show results for the servers in a dynamic server group as of the last time the group was reconciled.



In some cases, you might experience a delay between the time a modification is made in Opware and when it appears in your reports depending upon the way your Crystal Reports server has been configured. For information on how to troubleshoot this issue, see See Chapter 6, "Troubleshooting DCI Report Server" on page 79 of this guide for more information.

Change History Reports

This group of provides reporting on configuration backups and jobs run in the core.

• Configuration Backups by Server

- Report Description: This report shows the results of configuration backups run on a particular server during a defined time period. This report only includes triggered incremental and full backups. Manual backups are excluded. Tracked configuration applies to the policies that are directly attached to a server or through a node, regardless of whether or not the policies have been reconciled onto a server.
- Report Chooser: You can choose to search for configuration backups for specific servers by name, or for all servers in the core. You can also enter the number of days of history to examine.
- Reports Results: The results shows a list of all servers that have had configuration backups run during the time frame listed in your report criteria. For each configuration backup, you will see the time it was run, the type of configuration file or object that was backed up, and the type of backup (triggered, incremental, and so on). Clicking on the name of the server in the report will display details for that server.

The Group Tree (left side) arranges all servers that have had configuration backups run during the specified time frame. You can click the server link in the Group Tree in order to view that server's configuration backups.

• Configuration Backups by Server Group

- Report Description: This report lists the configurations that have been backed up for a particular public server group during a defined time period. This report only includes triggered incremental and full backups; manual backups are excluded. This report is the same as Backed Up Configurations by Server, except that the servers are displayed by server group. The configurations, however, are performed based on the policies defined at the server level, not the server group level. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.
- Report Chooser: You can choose to search for configuration backups for specific public server groups by name, or for all server groups in the core. You can also enter the number of days of history to examine.
- Reports Results: The results shows a list of all public server groups that have had configuration backups run during the time frame listed in your report criteria. If a

server belongs to more than one public server group, it will appear on the report under each of those server groups.

The Group Tree (left side of report) shows a list of all public server groups that have had configuration backups run during the days of history listed in your report criteria. To view details of an individual server group, click the server group link in the Group Tree, or the server name link on the main page of the report results.

- **Recent Jobs by Date**

- Report Description: This report lists all server jobs chronologically by date for a specific time period.
- Report Chooser: You can choose to search for either all jobs or a specific job type. You can also enter the number of days of history to examine.
- Reports Results: The results show all jobs run during the time frame specified, listed by operating system. Clicking on the name of a server job will show details for that job. The details for a job show each time the job was run, its start and stop time, its success or failure, and how many servers the job was run on. You can click further on a specific job detail to get more detailed information, and you can drill down to view properties of an individual server.

- **Recent Jobs by Server:**

- Report Description: This report lists all server jobs alphabetically by server name.
- Reports Results: The results show all servers that have had jobs run on them during the specified time frame, with a list of jobs shown beneath the server. Clicking on the name of a job will show that details for that job.

The Group Tree (left side of the report window) also displays each server in the report. Clicking a server name in this section will highlight that server and display the server's job details in the report window.

- **Recent Jobs by User:**

- Report Description: This report lists all server jobs alphabetically by the user name of the person who ran the job.
- Reports Results: The results show all jobs run during the specified time frame, arranged by the user who ran each job. Each job also shows the server it was run on. You can click on the name of a job to see details for that job, and you can also click the name of a server to view details about that server.

The Group Tree (left side of the report window) also displays each user that has

run a job in the report. Clicking a user name in this section will highlight that user and display that user's jobs in the report window.

- **Recent Patch Jobs**

- Report Description: This report displays the patches installed on servers grouped by operating system of the servers.
- Reports Results: The results show all patch jobs run during the time frame specified, listed by operating system. Clicking on the name of a server job will show details for that job. The details for a job show each time the job was run, its start and stop time, its success or failure, and how many servers the job was run on. Click the server name (listed under “hostname”) for further details on that server.

Servers, Facilities, and Customers

This group of reports provides reporting on servers, facilities, and customers.

- **All Servers by Facility**

- Report Description: This report shows all managed servers that are located in each Facility in the core. This includes those servers in the server pool, but not those servers that do not yet have an OS provisioned on them and are not in full production. Servers that have been deactivated also do not appear in this report.
- Reports Results: The results display a bar graph that shows all facilities and the number of servers in each. Click on a Facility in the graph to show graphs of all servers arranged by OS in that facility. Then, click the name of an OS to show the selected servers arranged by Customer. Click once again on a customer to view a list of all servers that belong to that customer. Click the server name to view details on the server's properties.

- **Managed Servers by Facility**

- Report Description: This report shows all managed servers in the core organized by Customer. This report will show only managed servers, and not any servers in the server pool.
- Reports Results: The results display a bar graph that shows all facilities and the number of managed servers in each. Click on a Facility in the graph to show the list of graphs of all managed servers arranged by OS in that facility. Then, click the name of an OS to show the selected managed servers arranged by Customer. Click once again on a customer to view a list of all managed servers that belong to that customer. Click the managed server name to view details on the server's

properties.

- **Nodes by Customer:**

- Report Description: This report lists all software nodes that are attached to servers, grouped by customer. The report lists each software node, the server it is attached to, and the customer that the server belongs to.
- Reports Results: The main page of the results displays an alphabetical list of each software node, the server it is attached to, and the customer that the server belongs to. The Group Tree (left side) shows a list of all software nodes that can be clicked to jump to the software node in the report. When clicked, the software node will be highlighted in the main report results page. Click the server the node is attached to in order to view more detailed server property information.

- **Server Pool**

- Report Description: This report lists servers in the server pool (unprovisioned servers without an operating system installed) grouped by Facility.
- Reports Results: The results display a bar graph showing all servers in the server pool for each facility in the core, including the number of managed servers in each. Click on a facility in the graph to show the list of graphs of all servers in the server pool in that facility, arranged by OS. Then, click the name of an OS to show the selected server pool servers arranged by Customer. Click once again on a customer to view a list of all server pool servers that belong to that customer. You can click the managed server name to get details on the server's properties.

- **Servers by Customer**

- Report Description: This report lists how many servers are assigned to each Customer.
- Reports Results: The results display a bar graph that shows all customers in the core and the number of managed servers in each. Click on a customer in the graph to show the list of graphs of all managed servers arranged by OS in that customer. Then, click the name of an OS to show the selected managed servers arranged by Customer. Click once again on a customer to view a list of all managed servers that belong to that customer. You can click the managed server name to view details on the server's properties.

To toggle between facilities, use the main report toggle (drop down list next to the print icon).

Software and Patch Policies

This group of reports provides reporting on software, audit, and patch policies.

- **Server Attachments by Node**

- Report Description: This report lists all each node attached to servers, grouped by software node name.
- Reports Results: The results list all nodes in the software tree by software node type, beginning with application servers. Under each node in the report, all servers that are attached to that node are listed, showing the server's IP, OS, and facility and customer assignments, if any. You can click the server name to view detailed server property information.

The Group Tree (left side of the report window) displays all node categories. Click a category to jump to the selected node, which will display in highlighted text on the main report page.

- **Server Groups without Application Configuration Policies**

- Report Description: This report alphabetically lists all public server groups without application configuration policies, including the number of servers in each public server group and each group's parent path.
- Reports Results: Each public server group is shown with a count of how many servers it contains. Clicking the number in the Server Count column will display the individual servers in a group. Click the server name on this page to view detailed server property information. If a server belongs to more than one public server group, it will appear on the report under each of those server groups.

- **Server Groups without Compliance Audit Policies**

- Report Description: This report alphabetically lists all public server groups that are without compliance audit policies, including the number of servers in each public server group and each group's parent path.
- Reports Results: Each public server group is shown with a count of how many servers it contains. Clicking the number in the Server Count column will display the individual servers in a group. Click the server name on this page to view detailed server property information. If a server belongs to more than one public server group, it will appear on the report under each of those server groups.

- **Server Groups without Configuration Tracking Policies**

- Report Description: This report alphabetically lists all public server groups that are

without configuration tracking policies, including the number of servers in each group and each group's parent path. Tracked configuration applies to the policies that are directly attached to a server or by a node, regardless of whether or not the policies have been reconciled onto a server.

- Reports Results: Each public server group is shown with a count of how many servers it contains. Click the number in the Server Count column to display the individual servers in a group. Click the server name on this page to view detailed server property information. If a server belongs to more than one public server group, it will appear on the report under each of those server groups.

- **Server Groups without Patch Policies**

- Report Description: This report alphabetically lists all public server groups that are without patch policies, including the number of servers in each public server group and each group's parent path.
- Reports Results: Each server group is shown with a count of how many servers it contains. Click the number in the Server Count column to display the individual servers in a group. Click the server name on this page to view detailed server property information. If a server belongs to more than one public server group, it will appear on the report under each of those server groups.

- **Server Groups without Software Policies**

- Report Description: This report alphabetically lists all server groups that are without Software policies, including the number of servers in each public group and each group's parent path.
- Reports Results: Each public server group is shown with a count of how many servers it contains. Click the number in the Server Count column to display the individual servers in a group. Click the server name on this page to view detailed server property information. If a server belongs to more than one public server group, it will appear on the report under each of those server groups.

- **Servers without Application Configuration Policies**

- Report Description: This report alphabetically lists all servers without application configuration policies.
- Reports Results: Each server is listed in alphabetical order, and includes such server information as customer, facility, operating system, and use. Click the server name on this page to view detailed server property information.

- **Servers without Compliance Audit Policies**

- Report Description: This report alphabetically lists all servers without compliance audit policies.
- Reports Results: Each server is listed in alphabetical order, and includes each server information as its customer, facility, operating system, and use. Click the server name on this page to view detailed server property information.

- **Servers without Configuration Tracking Policies**

- Report Description: This report alphabetically lists all servers without configuration tracking policies. Tracked configuration applies to the policies that are directly attached to a server or through a node, regardless of whether or not the policies have been reconciled onto a server.
- Reports Results: Each server is listed in alphabetical order, and includes each server information as its customer, facility, operating system, and use. Click the server name on this page to view detailed server property information.

- **Servers without Patch Policies**

- Report Description: This report alphabetically lists all servers without patch policies.
- Reports Results: Each server is listed in alphabetical order, and includes each server information as its customer, facility, operating system, and use. Click the server name on this page to view detailed server property information.

- **Servers without Software Policies**

- Report Description: This report alphabetically lists all servers without Software policies.
- Reports Results: Each server is listed in alphabetical order, and includes each server information as its customer, facility, operating system, and use. Click the server name on this page to view detailed server property information.

- **Software by Customer**

- Report Description: This report shows the software each customer should have according to the Model.

Reports Results: The results page shows an alphabetical list of all customers, with a count of total servers for each customer. Click a the number to the left of the customer name to view a software list for that customer, then click a software name to see more specifics information about the software nodes and their

attached packages.

Software and Patch State

This group of reports provides reporting on the state of software and patches in your facility.

- **Compliance Dashboard**

- **Report Description:** This report summarizes compliance versus non-compliance for all servers in the core. A server is considered non-compliant if it is missing any modeled software application or patch or if it has failed any application configuration or compliance test audits. Audit results include those occurring over the last 30 days.
- **Reports Results:** The first page of the results display a bar graph showing all compliant (green) and all non-compliant (red) servers, including the number of servers for each. Clicking on the bars will display a list of all servers in each category, and includes each server's customer, facility, OS, overall compliance (no-red or yes-green), and includes a Installed/Expected Software Nodes, Installed/Expected Patches, Matching/Audited Configuration (Applications), Backed Up/Tracked Configuration Objects, and Matching/Total Compliance Audits.

For a more comprehensive view of a specific server's compliance, click the server name link. This level of the report (which will likely span several pages) provides a very detailed report of all the compliance categories.

For example, the Software Node section provides a summary count of installed/expected nodes, and is followed by a list of all software nodes expected to be installed on the server, with those nodes not installed highlighted in red. In the Patch Compliance Details section (you might need to click the right arrow button to view the page), the top of the section provides a summary of how many patches are installed and how many are expected. The following section lists each patch by name and highlights in red the ones that are expected but not installed on the server.

The Application Configuration Audits for the Past 30 Days section presents a summary of all application configuration audits run on the server and the number of audits that failed. The following section lists each audit by job ID and provides the application name, the differences found between the application configuration and the actual file on the server, and the name of the file where the discrepancy is found.

In the Configuration Backups for the past 30 Days section, the report results

display a list of all successful configuration backups within the last 30 days, including the time of the backup, the source, the backup type (triggered, full, incremental), and the configuration that was backed up.

In the Compliance Audits for the Past 30 Days section, the report displays all compliance audits and that were run in the past 30 days and indicates their success or failure. Those compliance audits that failed are highlighted in red. Each audit is listed by job ID, and includes its start time, length of time it took to run the audit, the compliance test name, success or failure (Audit Status), and the source of the audit.

- **Compliance Summary**

- Report Description: This report summarizes and presents an overview of servers and/or server groups that are in compliance with their policies according to user-defined maximum compliance thresholds. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.

Compliance is determined by judging how the software on the actual server in a server group matches the software defined for the server in the Opware model. For each server, the Compliance Summary Report checks the following: Installed/Expected Software Nodes, Installed/Expected Patches, Matching/Audited Configuration (Applications), Backed Up/Tracked Configuration Objects, and Matching/Total Compliance Audits.

This report rates a server's compliance according to three levels: green (compliant), yellow (potentially non-compliant), and red (non-compliant) based upon how well the server rates in each of these categories in comparison to the Opware model.

By default, Green has non-compliance of 5%. This mean that for each server group, the report will mark as green those servers that are that are within 5% of compliance for each of the compliance categories overall compliance, installed/expected software, Installed/Expected Patches, and so on.

Yellow has non-compliance of greater than 5% but no more than 10%. Red has non-compliance of greater than 10%.

The report results are calculated according to the following formula:

A = installed software + installed patches + matching configurations + matching compliance audits

B = expected software + expected patches + audited configurations + total

compliance audits

Overall Compliance = $((B-A)/B) * 100$

- Report Parameters: First choose whether to list server groups, ungrouped servers, or specific server groups by name. Then, in the Days of Audit History section, choose the number of days for which you want to generate results.

In the Compliance levels section choose which thresholds levels to include in the report: green, yellow, red, or all. This report will search and arrange groups of servers according to the non-compliance threshold set for each colored level.

- Reports Results: The first page of the results displays an alphabetical list of all server groups found according to the set criteria. All servers that meet the green compliance standard will be highlighted in yellow; and those servers above the yellow compliance standard will be highlighted in red.

For a more comprehensive view of a specific server's non-compliance, click the server name link. This level of the report (which will likely span several pages) provides a very detailed report of all the non-compliance categories.

For example, the top of the Software Node section provides a summary count of installed/expected nodes, and is followed by a list of all software nodes expected to be installed on the server, with those node not installed highlighted in red. In the Patch Compliance Details section (you might need to click the right arrow button to view the page), the top of the section provides a summary of how many patches are installed and how many are expected. The following section lists out each patch by name and highlights in red the ones that are expected but not installed on the server.

In the Application Configuration Audits for the Past Days section, you see a summary of all application configuration audits run on the server and the number of audits that failed during the number of days specified in the report parameters. The following section lists each audit by job ID and provides the application name, the differences found between the template and the actual file on the server, and the name of the file where the discrepancy is found.

In the Configuration Backups for the past 30 Days section, the report results display a list of all successful configuration backups within the last 30 days, including the time of the backup, the source, the backup type (triggered, full, incremental), and the configuration that was backed up.

In the Compliance Audits for the Past 30 Days section, the report displays all compliance audits and that were run in the past 30 days and indicates their

success or failure. Those compliance audits that failed are highlighted in red. Each audit is listed by job ID, and includes its start time, length of time it took to run the audit, the compliance test name, success or failure (Audit Status), and the source of the audit.

- **Configuration Audits by Server**

- Report Description: This report displays detailed application configuration audit results by server within a user defined time period.
- Report Chooser: You can choose to search for application configuration audits for all servers, or specific server (by name) in the core. To search for a specific server by name, enter the in the Server name field. By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all application configuration audits by job ID. Those application configuration audits that failed are highlighted in red, while those that passed are in white. For each audit that failed, the report lists how many files were found with discrepancies between the application configuration and the actual file on the server and the files where the discrepancies were found. To view a specific application configuration job, you can click the job ID. To view detailed server property information, click the name of the server.

The Group Tree (left side of the report window) shows a list of all servers that were found by the report. Click any server to view all application configurations audits run for that server.

- **Configuration Audits by Server Group**

- Report Description: This report displays detailed application configuration audit results by public server group within a user defined time period.
- Report Chooser: You can choose to search for application configuration audits for all public server groups, or specific public server group name in the core. To search for a specific public server group by name, enter the in the Server group name field. By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all application configuration audits by public server group. (If a server belongs to more than one public server group, it will appear on the report under each of those server groups.) Each public server group lists all servers in the group, and for each server, all application configuration

audits run are displayed by order of job ID.

Those application configuration audits that failed are highlighted in red, while those that passed are in white. For each audit that failed, the report lists how many files were found with discrepancies between the application configuration and the actual file on the server and the files where the discrepancies were found. To view a specific application configuration job, you can click the job ID. To view detailed server property information, click the name of the server.

The Group Tree (left side of the report window) shows a list of all servers that were found by the report. Click any server to view all application configurations audits run for that server.

- **Difference Audits by Server**

- Report Description: This report presents the results of compliance audits run on a particular server during a defined time period.
- Report Chooser: You can choose to search for server compliance (difference) audits for all servers, or specific server (by name) in the core. To search for a specific server by name, enter the name in the Server name field. By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all server compliance difference audits by job ID. Those server compliance audits that failed (differences between servers were found) are highlighted in red, while those that passed (did not find any differences) are in white. Each audit for a server is listed by job ID, and includes job start time, elapsed time, name of the test (audit), and the audit source (server name).

In the Differences Found column, the report lists how many differences were found with discrepancies between the application configuration and the actual file on the server and the files where the discrepancies were found. To view detailed server property information, click the name of the server.

The Group Tree (left side of the report window) shows a list of all servers that were found by the report. Click any server to view server compliance difference audits run for that server.

- **Difference Audits by Server Group**

- Report Description: This report presents the results of compliance audits run on a particular public server group during a defined time period. This report is the same

as Difference Audits by Server, except that the servers are displayed by public server group. The audits, however, are performed based on the policies defined at the server level, not the server group level.

- Report Chooser: You can choose to search for server compliance (difference) audits for all public server groups, or specific public server groups (by name) in the core. To search for a specific public server group by name, enter the name in the Server name field. By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all public server groups and the servers within them that have had compliance difference audits run. (If a server belongs to more than one public server group, it will appear on the report under each of those server groups.) Each public server group shows a list of all servers in it, and for each server in the group the report lists all server compliance (difference) audit information, sorted by job ID.

Those server compliance audits that failed (differences between servers were found) are highlighted in red, while those that passed (did not find any differences) are in white. Each audit includes job ID, job start time, elapsed time, name of the test (audit), and the audit source (server name).

In the Differences Found column, the report lists how many differences were found with discrepancies between the application configuration and the actual file on the server and the files where the discrepancies were found. To view detailed server property information, click the name of the server.

The Group Tree (left side of the report window) shows a list of all public server groups that had server compliance (difference) audit tests run. Click any server groups to view server compliance difference audits run for that groups.

- **Package Catalog**

- Report Description: This report lists the packages installed on each server arranged by operating system.
- Report Chooser: By default, this report will search all operating systems. However, you can specify a specific operating system from the Operating system drop down list.
- Reports Results: The results display all known software, grouped alphabetically. Drill down by the first letter of the software package name and then click to see a list of servers that have that software installed. To view detailed server property

information, click the name of the server.

The Group Tree (left side of the report window) also shows an alphabetical list of first letters for software names. You can expand the letters and click links for the specific software names and view the servers this software is installed on.

- **Patching Audits by Server**

- Report Description: This report displays a summary of the patches expected on a server versus the patches actually on a server. (Software is not listed.)
- Report Chooser: You can choose to search for all servers in a core or a specific server name. To search for a specific server by name, enter the name in the Server name field.
- Reports Results: The results display a list of all servers that have had patch audits run on them. For each server, the report shows a list of all patches expected to be installed on the server. Those patches that are installed are shown in white, while those patches expected but not installed on the server are highlighted in red. For each patch, the reports lists the patch number, the node it belongs to in the Opsware model, the patch type, the file name, the description and a status of installed or not. To view detailed server property information, click the name of the server.

The Group Tree (left side of the report window) shows a list of all servers found in the report. Click a server in this section to jump directly to that server.

- **Patching Audits by Server Group**

- Report Description: This report displays a summary of the patches expected on all servers in a public server group versus what is actually on the servers. (Software is not listed.) This report is the same as Patching Audits by Server, except that the servers are displayed by server group. The audits, however, are performed based on the policies defined at the server level, not the server group level.
- Report Chooser: You can choose to search for all public server groups in a core or a specific public server group name. To search for a specific server by name, enter the name in the Server name field.
- Reports Results: The results display a list of all public servers groups with servers that have had patch audits run on them. (If a server belongs to more than one public server group, it will appear on the report under each of those server groups.) For each server in a group, the report shows a list of all patches expected to be installed on the server. Those patches that are installed are shown in white,

while those patches expected but not installed on the server are highlighted in red. For each patch, the reports lists the patch number, the node it belongs to in the Opsware model, the patch type, the file name, the description and a status of installed or not. To view detailed server property information, click the name of the server.

The Group Tree (left side of the report window) shows a list of all public server groups found in the report. Click a server group in this section to jump directly to that server group

- **Patch Catalog**

- Report Description: This report lists the patches installed on each server limited by operating system.
- Report Chooser: You can choose to view all patches for all operating systems, or limit the search by specific operating system using the Operating system drop down list.
- Reports Results: The results display all known patches, grouped alphabetically. For each operating system, the report lists the number of patches found. Click the number to view a list of all patches for an operating system. The patch by operating system list shows how many servers have the selected patch installed. Click the number to the left of the patch name to view a list of servers using the patch. Click the server name link to view more detailed server property information.

- **Patch Inventory**

- Report Description: This report lists all servers in a core and the patches installed on each server.
- Reports Results: The results display a list of all servers in the core, showing servers with patches on them. Each server with patches has a number shown in the Number of Patches column. Click the number of patches and the report displays a list of all patches on the server, when each patch was installed, the name of each patch, and patch type.

- **Software Audits by Server**

- Report Description: This report displays a summary of software expected on a server versus the software actually installed. Only software is listed, not patches.
- Report Chooser: You can choose to view software audits run on all servers, or search for a specific server by name from the Server name drop down list.
- Reports Results: The results display a list of all servers and the software packages

installed on them. For each software package, the report indicates the number of software packages expected and the number expected but not installed. Those software packages that are expected to be installed but are not will be highlighted in red. To view more detailed information about a server, click the server name link.

The Group Tree (left side of the report window) shows a list of all servers found in the report. Click a server in this section to jump directly to that server.

- **Software Audits by Server Group**

- Report Description: This report shows a summary of software expected on a servers versus the software actually installed, arranged by public server group. Only software is listed, not patches. This report is the same as Software Audits by Server, except that the servers are displayed by server group. The audits, however, are performed based on the policies defined at the server level, not the server group level.

- Report Chooser: You can choose to view software audits run on all public server groups in the core, or search for a specific public server group by name from the Server group name drop down list.

- Reports Results: The results display a list of all server groups and the software packages installed on the servers within them. (If a server belongs to more than one public server group, it will appear on the report under each of those server groups.) For each software package, the report indicates the number of software packages expected and the number expected but not installed. Those software packages that are expected to be installed but are not will be highlighted in red. To view more detailed information about a server, click the server name link.

The Group Tree (left side of the report window) shows a list of all public server groups found in the report. Click a server group in this section to jump directly to that server

- **Software Inventory**

- Report Description: This report lists a software inventory grouped by customer.

- Reports Results: The first page displayed of the results shows a list of customers in your core. Click a customer to view an alphabetical list of all software associated with the customer. To view the servers that are using the software, click one of the software links. A page showing the name of the software and all servers that have the selected software installed appears. To view more detailed information about a server, click the server link name.

Users and Security

This group of reports provides reporting in users, user groups, and permissions.

• **User Groups**

- Report Description: This report lists the members, features and permissions associated with a specified user group.
- Report Chooser: Specify a user group name to search for, or leave the User group name field with a * to search for all user groups.

Reports Results: The results page displays an alphabetical list of user group names, including all member of the group, their full name, the most recent time they logged in, and their email. Below the list of users in each user group is a list of all the features associated with the group. If the information for a group is too long to fit on the page, then click the right arrow key at the top or bottom of the page to see more information.

The Group Tree (left side of the report window) shows all the user groups in the core, so if you want to navigate to a specific user group not shown on the first page of the results, select a user group from this section and the results will jump directly to information on that group.

• **User Logins**

- Report Description: This report shows what a list of all users who have logged into the core, sorted by most recent user login. This report is useful to find out which users are active and which users have not logged in to the core in a long time. The values for determining a user status are:

Expired: Users who have not logged in for more than 90 days.

Warning: Users who have not logged in for between 60 to 90 days.

Active: Users who have logged in within the past 60 days.

Unknown: Users whose last login date is not known.

- Report Chooser: Click the OK button if you would like to run the report to see all users activity who have logged in the last 60 days, and those users who have not logged in during the last 90 days. All users who have logged in during the last 60 days will be grouped as “active,” while users who have not logged in for at least 90 days will be grouped as “expired.”

To specify a different threshold for viewing recent user logins, in the Active Threshold field, enter the maximum number of days since the most recent login; in the Warning Threshold field, enter the maximum number of days since the most

recent login for a user.

- Reports Results: The results will display groups of users according to their user status criteria. The Group Tree (left side of the report window) shows the user status categories, which you can click to display each category.
- **User Permissions:** This report describes what permissions are assigned to a particular user.
 - Report Description: This report lists the members, features, and permissions associated with a specified user group.
 - Report Chooser: Click OK to generate a report listing all users permissions, or enter a specific user name in the user name field.
 - Reports Results: The results display an alphabetical list of all users found in the report, including their permissions. The Group Tree (left side of report window) displays a list of all users found in the report. Click a user name to view that user's permission information.

Network Reports

The following networking reports are available when the Opsware Network Automation System (NAS) is also installed.

Network Reports consist of the following report categories:

- Device Status
- Tasks
- Workflow
- Policies and Rules
- Users and Rules

Device Status

This group of reports provides reporting on the status of devices managed by the NAS server.

- **Active Configurations**
 - Report Description: This report displays all active device configurations in the NAS environment.
 - Reports Results: The results display a complete list of all active device configurations, arranged alphanumerically by hostname. For each configuration,

the reports includes device host name, the date it was last modified, the user who made the modification, and any comments.

- **Configuration Changes**

- Report Description: This report shows the configuration changes that have occurred in a user-defined time range.
- Report Chooser: By default the report will search for device configuration changes over a period of 30 days. To change this time frame, enter a number in the Days of history field.
- Reports Results: The results displays a list of all devices that have had a configuration change within the time frame specified in the report chooser. The list is organized by chronological order starting with the most recently changed devices. Each change shows the date and time it was change, the user who made the change, and any comments.

- **Device List**

- Report Description: This report presents a complete list of all devices available in the network inventory.
- Reports Results: The results display a list of all devices in the NAS network inventory, arranged alphanumerically by hostname. For each device, the reports shows the hostname, device IP, vendor, model, and the date when the device configuration was last changed.

- **Devices with Different Startup and Running Configurations**

- Report Description: This report lists devices with a start up configuration that is different than their running configuration.
- Reports Results: The results display a list of all devices in the NAS environment that have startup configurations different than their running configurations. Each device is listed according to when its configuration was changed, starting with the most recent. For each device, the report shows hostname, IP address, vendor, model number, and date last changed.

- **Devices with Driver Assigned but No Configuration Stored**

- Report Description: This report lists all devices with a driver assigned but that do not have a configuration stored.
- Reports Results: The results display a list of all devices that have a drivers assigned to them but do not have a configuration stored. For each device, the

report shows host name, IP address, vendor, model number, and date last changed. Devices shown in red text failed their most recent snapshot attempt.

- **Devices without Driver Assigned**

- Report Description: This report lists all devices without any driver assigned.
- Reports Results: The results display a list of all devices that do not have a driver assigned, and includes the hostname and device IP.

- **Diagnostics**

- Report Description: This report shows all diagnostics that have been run in a user-defined time range.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all diagnostics run in your NAS environment within the time frame specified in the report parameters, sorted chronologically with the most recent diagnostic listed first. Each entry lists the hostname of the device on which the diagnostic was run, the date and time of the diagnostic, and the diagnostic type.

- **Duplicate IP Addresses**

- Report Description: This report lists all duplicate IP addresses in the NAS environment.
- Reports Results: The results display a list of all duplicate IP addresses in the NAS environment, including the host names of the devices.

- **Inaccessible Devices**

- Report Description: This report displays a list of devices with access failures.
- Reports Results: The results display a list of all devices in the NAS environment that are inaccessible. For each device, the results list its hostname, device IP, vendor, model, date and time the device's configuration was last changed, and its current status (active or inactive). Devices shown in red are those that failed their most recent snapshot.

- **Inactive Devices**

- Report Description: This report lists all inactive devices in the network inventory.
- Reports Results: The results display a list of all devices in the NAS environment

that are inactive, and includes each device's hostname, device IP, vendor, model, date and time the device's configuration was last changed.

- **Modules**

- Report Description: This report lists the modules available in the network device inventory as well as slot info and descriptions for each.
- Reports Results: The results display a list of all available modules in your NAS environment and lists each module's hostname, slot, description, model, and serial number.

- **Port Availability**

- Report Description: This report lists devices that have port availability of less than ten percent.
- Reports Results: The results display a list of all devices in your NAS environment that have a port availability of less than 10 percent. For each device, the result displays its hostname, IP address, management status (active or inactive), vendor, model number, date the device's configuration was last changed, and the number of free ports on the device.

- **Sessions Created**

- Report Description: This report lists what telnet/ssh proxy sessions have been created within a user-specified time range.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all telnet/ssh proxy sessions that have occurred within the time frame specified in the report parameters. For each session, the results list the device's hostname, IP address, the start and end time of the session, the current status of the session (open or closed), session type (telnet or ssh), and the user that created the session.

Tasks

This group of reports provides reporting on tasks run in your NAS environment.

- **Event List**

- Report Description: This reports displays all NAS events over a user-defined period of time.

- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field. You can choose by default to search for all tasks run on all device groups, or specify a group name in the Device group field.
- Reports Results: The results display a list of all events that occurred in your NAS environment within the time frame specified in the report parameters. For each event, the results list the time and date, a summary of the event (for example, “Device Snapshot”), the host name of the device the event occurred on, the device’s IP address, and the user who initiated the event.

- **Failed, Skipped, and Duplicate Tasks**

- Report Description: This report shows what tasks have failed, been skipped, or duplicated within a user-defined time period.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all tasks that have failed, were skipped, or duplicated within the time frame specified in the report parameters. For each failed, skipped, or duplicated task, the results list date and time, the name of the task, host or group on which the task was performed, any comments entered by the user who initiated or scheduled the task, the name of the user, and the status (for example, “failed”).

- **Past Tasks**

- Report Description: This report displays all device change tasks performed within a user-defined time range.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all device change tasks that occurred within the time frame specified in the report parameters. For each task, the results list the date and time the task change occurred, the host or group affected, the user who scheduled the task, the task type, the status of the task (for example, succeeded or failed, and any user-entered comments.

- **Pending Deployments**

- Report Description: This report displays all scheduled software deployments within

a user-defined time range.

- Report Chooser: By default, the report will return results for pending deployments for 30 days into the future, but you can change the time period searched by entering a new value in the Future days field.
- Reports Results: The results display a list of all pending deployment tasks. For each pending deployment, the report lists the date and time the deployment was scheduled, the host/group name the task affects, the user who scheduled the deployment, the status of the task, and any comments.

- **Pending Tasks**

- Report Description: This report lists all device change tasks scheduled for a user-defined time range.
- Report Chooser: By default, the report will return results for pending tasks for 30 days into the future, but you can change the time period searched by entering a new value in the Future days field.
- Reports Results: The results display a list of all pending tasks. For each pending task, the report lists the date and time the task was scheduled, the host/group name the task affects, the user who scheduled the task, the task type, the status of the task, and any comments.

Workflow

This group of reports provides reporting on workflow and tasks in your NAS environment.

- **Approved Changes**

- Report Description: This report lists all tasks approved within a user-defined time range.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all tasks that were approved for change within the time frame specified in the report parameters. For each task, the results list the date and time the task was run, the host or group the task was run on, the user who scheduled the task, the task type, the status of the task (for example, failed or succeeded), and any comments.

- **Changes Pending Approval**

- Report Description: This report lists the changes (tasks) pending approval as well

as who scheduled the change and the host or group affected.

- Reports Results: The results display a list of all changes that are pending approval, including the date and time the task was initiated, the task name, the host/group the task affects, any comments, the user who initiated the task, and the task's status.

- **Task that Require Approval**

- Report Description: This report lists all tasks that require approval within a user-defined time range.
- Report Chooser: By default, the report will return results for scheduled tasks that require approval for 30 days into the future, but you can change the time period searched by entering a new value in the Future days field.
- Reports Results: The results show a list of all task that are scheduled within the time frame specified in the report parameters, including the scheduled date and time, the host/group name the task affects, the user who scheduled the task, its approval status, and status.

- **Unapproved Changes**

- Report Description: This report shows what unapproved changes have taken place in the network environment within a user specified time range.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all unapproved changes that occurred within the time frame specified in the report parameters. For each unapproved change that occurred, the results list the date and time of the change, the type of task that was run, any comments, the user who scheduled the task, and the status of the task (for example, failed or succeeded).

Policies and Rules

This group of reports provides reporting on all policies and rules related to your managed devices.

- **ACL Changes**

- Report Description: This report lists all Access Control List (ACL) changes in the last seven days and the specific devices the changes occurred on.
- Reports Results: The results display a list of all ACL changes that occurred on

devices in your NAS environment, including for each device: host name, ACL Id, handle, type of ACL, and the date and time of the last modification.

- **ACLs in Use**

- Report Description: This report shows all ACLs that are in use for specified devices.
- Reports Results: The results display a list of all ACLs in use on devices in your NAS environment. For each device, the results list its host name, ACL Id, handle, type of ACL, and the date and time of the last modification.

- **All ACLs**

- Report Description: This report lists the details of all the ACLs in the inventory.
- Reports Results: The results display a list of all ACLs in your NAS environment device inventory. For each device, the results list its host name, ACL Id, handle, type of ACL, and the date and time of the last modification.

- **Configuration Policies**

- Report Description: This report displays all configuration policies and status in place in the network environment.
- Reports Results: The results display a list of all configuration policies in your NAS environment, and includes the policy name, a description, and status (active or inactive).

- **Configuration Policy Events**

- Report Description: This report lists all configuration policy non-compliance events within a user-defined time range.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all configuration policy events that occurred within the time frame specified in the report parameters. For each event, the results display its date and time, a summary of the event, the policy name, the device IP where the event occurred, and its host name.

- **Device Password Rules**

- Report Description: This report lists all password rules in place in the network

environment.

- Reports Results: The results display a list of all device password rules in place in your NAS environment. For each password rule, the report displays when the rule was last changed, the password rule name, its type, name of the rule, and the user who modified the rule.

- **Device Software Report**

- Report Description: This report lists what devices are in software compliance.
- Reports Results: The results display a list of all devices in your NAS environment that are in software compliance, showing each device's host name, device IP, software version, change date, its compliance, any comments, image set name, and who made the change (if applicable).

- **Policy Rule Violation**

- Report Description: This report lists all policy rules that have been violated over a specified time period.
- Report Chooser: By default, the report will return results for the last 30 days, but you can change the time period searched by entering a new value in the Days of history field.
- Reports Results: The results display a list of all policy rule violations that have occurred over the time frame specified in the report parameters. For each violation, the report lists: the date and time of the violation, a summary, the policy name that was violated, the device IP where the violation occurred, and the device host name.

Users and Rules

This group of reports provides reporting on users and policy rules in your NAS environment.

- **Network Status Report**

- Report Description: This report shows the status of devices in the network.
- Reports Results: The results display a list of all network status categories in your NAS environment, including policy rule violations, start up versus running configuration mismatches, software compliance violations, device access failures and configuration changes within the past 24 hours.

To drill down to more specific information in each category, click the category section. After you click a section, you will see a list of device host name that you

can click to find the device in the report results.

- **Users List**

- Report Description: This report presents a list of all users in the network environment.
- Reports Results: The results displays a list of all users in the NAS environment, including each user's login name, first and last name, email address, and current status.

Compliance Center

Several compliance standards have become commonplace in the IT industry. DCI supports reporting for these specific standards. Some background for each of these four compliance standards is provided in the following sections.



The Opsware Compliance Center is based on Opsware's understanding of the regulations and standards presented. Opsware is not an auditor or legal authority, and you should consult your corporate auditor or legal representative for guidance.

COBIT

Control Objectives for Information and related Technology (COBIT), published by the IT Governance Institute, is an internal control framework that helps meet the multiple needs of management by bridging the gaps among business risks, control needs, and technical issues and balancing risk versus return over IT and its processes. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT has been implemented by a number of companies to provide additional details about their system of IT controls.



Note that COBIT provides controls that address operational and compliance objectives in addition to those related directly to financial reporting.

COSO

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a landmark report on internal control. Internal Control – Integrated Framework provides a sound basis for establishing internal control systems and determining their effectiveness.

According to COSO, the three primary objectives of an internal control system are to ensure (1) efficient and effective operations, (2) accurate financial reporting, and (3) compliance with laws and regulations. The report outlines five essential components of an effective internal control system.

- **Control Environment:** This establishes the foundation for the internal control system by providing fundamental discipline and structure.
- **Risk Assessment:** This involves the identification and analysis by management - not the internal auditor – of relevant risks to achieving predetermined objectives.
- **Control Activities:** The policies, procedures, and practices that ensure management objectives are achieved and risk mitigation strategies are carried out.
- **Information And Communication:** This supports all other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allows people to carry out their duties.
- **Monitoring:** This covers the external oversight of internal controls by management or other parties outside the process or the application of independent methodologies such as customized procedures or standard checklists by employees within a process.

ITIL

IT Infrastructure Library (ITIL) was developed for the British government by the CCTA (now the OGC: Office of Government Commerce) and has been rapidly adopted across the world as the standard for best practice in the provision of IT services. Three major areas of ITIL are Service Support, Service Delivery, and Security Management. Service Support and Service Delivery are the disciplines that comprise IT Service Management (ITSM), which embraces provisioning and management of effective IT services.

- **Service Support**

Service Support is the practice of those disciplines that enable IT Services to be provided effectively. Service Support consists of six (6) disciplines:

- Configuration Management

- Incident Management
- Problem Management
- Change Management
- Service/Help Desk
- Release Management

- **Service Delivery**

Service Delivery is the management of the IT services themselves, and involves a number of management practices to ensure that IT services are provided as agreed between the Service Provider and the Customer. Service Delivery consists of five (5) disciplines:

- Service Level Management
- Capacity Management
- Continuity Management
- Availability Management
- IT Financial Management

- **Security Management**

Using security management, data and infrastructures are to be protected so that:

- Confidentiality is appropriately preserved
- Integrity of information is ensured.
- Availability is ensured.
- Conducting a transaction is not denied.
- Obligations imposed by law, contractual agreement, and supervisory bodies can be fulfilled.

Sarbanes Oxley (Section 404)

The Regulatory Compliance Center provides reports detailing the current compliance status of your network infrastructure with respect to Sarbanes-Oxley (Section 404) and supporting internal control frameworks. Sarbanes-Oxley (Section 404) itself provides no specific control requirements that can be used for IT-related compliance efforts.

Organizations must instead choose an internal control framework, such as COSO, COBIT, or ITIL, and enforce and report against that framework.

Overview

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as Sarbanes-Oxley, is designed to improve the accuracy and reliability of corporate disclosures to investors.

Sarbanes-Oxley generally applies to all U.S. companies registered with or required to file reports with the SEC (Securities and Exchange Commission). The regulation requires the CEO and CFO of reporting companies to certify their companies' SEC reports (with possible criminal and civil liability for false statements).

A key provision of Sarbanes-Oxley is Section 404, which specifically addresses internal control over financial reporting. Section 404 requires that reporting companies include an internal controls report and assessment as part of their financial reporting. Under the new compliance schedule released by the SEC on February 24, 2004, a company that is an "accelerated filer" as defined in Exchange Act Rule 12b-2 (generally, a U.S. company that has equity market capitalization over \$75 million and has filed at least one annual report with the Commission), must begin to comply with these amendments for its first fiscal year ending on or after Nov. 15, 2004 (originally June 15, 2004). A non-accelerated filer must begin to comply with these requirements for its first fiscal year ending on or after July 15, 2005 (originally April 15, 2005). (Refer to SEC Release No. 33-8392 for more detailed information.)

The consensus among auditors such as Deloitte & Touche, Ernst & Young, and PriceWaterhouseCoopers is that internal control over financial reporting includes controls over the safeguarding of assets and controls related to the prevention or timely detection of unauthorized acquisition, use, or disposition of an entity's assets (including network assets) that could have a material effect on the financial statements. IT support systems, including networks, are involved in the financial reporting process, and, as a result, should be considered in any design and evaluation of internal controls. Without adequate internal control over the network infrastructure, the reliability of the resulting financial reports cannot be assured.

Ensuring Compliance Using Opware

Sarbanes-Oxley Section 404 does not specify the means by which internal controls over the corporate IT infrastructure are to be established and verified. However, the SEC in its final rules regarding Sarbanes-Oxley made specific reference to the recommendations of the Committee of the Sponsoring Organizations of the Treadway Commission (COSO).

COSO issued a landmark report on internal control, Internal Control - Integrated Framework, which provides a sound basis for establishing internal control systems and determining their effectiveness.

The U.S. Public Company Accounting Oversight Board (PCAOB) is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002, to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports. The PCAOB emphasizes the importance of IT controls. Both the PCAOB and the SEC approved PCAOB Auditing Standard No. 2, titled An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements. PCAOB Auditing Standard No. 2 states: Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed due-process procedures to develop the framework. In the United States, the Committee of Sponsoring Organizations (COSO of the Treadway Commission has published Internal Control - Integrated Framework. COSO publication (also referred to simply as COSO) provides a suitable framework for purposes of management's assessment.

Often, SEC registrants and others have found that additional details regarding IT control considerations are needed beyond those provided in COSO. COBIT and ITIL have been implemented by a number of companies to provide additional details about their system of IT controls.

Custom Reports

Custom reports can be created and added depending on the specific needs of an operational environment. Using a Crystal Reports expert is recommended to create custom reports. See the DCI Administrator's Guide for more information.

Ad-hoc Reports

Ad Hoc Reporting enables searching for specific software, servers, and so on, grouped and filtered according to your needs. For example, the Servers folder allows for choosing the types of servers to include in the report and how the servers will be grouped.

To query a specific set of servers, limit the results to generate a smaller report of just the information you requested. The results first display summary graphs organized so that you can gather group information. Drill down to more detailed group information by clicking columns in the graph or links in the table until the actual server information that makes up

the summary is displayed. However, to display just a list of servers, select **List Only** and the report will suppress the graphs and show all the results in one long report. This format is best for printing or exporting an inventory list.

Chapter 4: Writing Custom Reports

IN THIS CHAPTER

This chapter discusses the following topics:

- Understanding Access to Public Views
- Using a Shipped Report to Create a Custom Report
- Extending Reports with other Data Sources
- Installing a Customized Report
- Sample def.xml file

Understanding Access to Public Views

Opware SAS keeps records of many events and items. Much of this data is available to create your own reports, or to integrate this information with other systems. The primary view of this information is called the Opware Public Views. It is a set of tables stored in a database. With the right information, you can establish a connection to the database and view this read-only information. Please refer to Appendix A: Public Views of this guide for detailed information about these tables.

You might want to create custom versions of our shipped reports, create your own reports, or create database connections to other systems. This chapter gives you an overview of the data in the public views and shows you how to understand and use it to create your own reports.

Using a Shipped Report to Create a Custom Report

The reports are created and processed with Crystal Reports, Report Application Server 10 (RAS). This software is not included with the DCI Report Server and must be purchased separately from Business Objects (<http://www.businessobjects.com/products/reporting/>

crystalreports/default.asp). This software allows you to edit .rpt files. You can copy any existing report from the report server located in the %SystemDrive%\Program Files\Opware\DCI\wwroot\Reports folder as your starting point.

If you are unfamiliar with Crystal Reports, ask Opware Professional Services for assistance.

The reports take advantage of an Open Database Connectivity (ODBC) connection to the Opware Oracle database, which can be seen on the System DSN tab, in the Start Menu ► Settings ► Control Panel ► Administrative Tools ► Data Sources (ODBC) on a Windows 2000 computer.

The database is accessed through the Public Views of the Model Repository. The Model Repository contains the tables listed in Appendix A of this guide. These tables can be used to generate new reports. The existing reports take advantage of the RAS Server for dynamically generating the correct report based on the input from the forms on the report server home page. Use of the report server API is not necessary to create reports but it does create a cleaner user interface. Consult the RAS documentation installed on the report server for more information about how to use the API (see the Start ► Programs ► Crystal Enterprise 9 ► Documentation menu).



Editing any of the reports that are shipped with the report server is not recommended. Doing so will result in losing these reports when you upgrade. To enhance an existing report, make a copy of the report, edit it, and place the finished file in the Custom folder. All existing reports contain special functions and parameters that the DCI home page uses. These functions and parameters should be removed from any customized reports to streamline custom reporting.

Extending Reports with other Data Sources

Crystal Reports allows one report to connect and relate to more than one data source. With the correct key fields, a report developer can create reports that combine the Opware data source with other data sources that might contain more detailed server information, cost or depreciation information, or application tracking information.

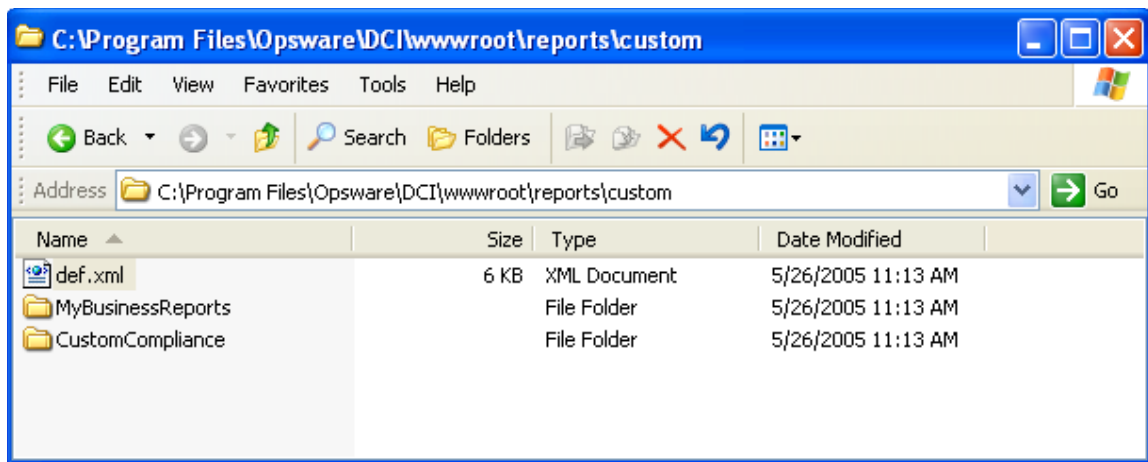
Installing a Customized Report

Custom reports should be placed put in either the custom folder or in a sub folder directly under custom folder. For example

```
%SystemDrive%\Program Files\Opware\DCI\wwwroot\reports\custom
```

If report filenames are suitable for display in DCI then no extra step is needed outside of placing the file in the folder. However, to have DCI display different names for the reports or folders, the def.xml file must be configured in the folder with the reports. (See the def.xml sample file for details)

Figure 4-1: Adding a New Report to the Custom Reports Folder



In addition to having the file name automatically appear on the home page, the Custom Report section can be configured to show a more descriptive name for a report, subsection names (for the left and right columns), a title for the section, and reorder the reports in the left and right columns.

Alphabetical order is the order they will appear on the home page. Reports in the Custom folder that do *not* have an entry in the configuration file will *not* appear on the home page.



You can use HTML tags in the configuration file to change the appearance of the labels for the reports, but make sure you use valid HTML tags, or it might affect the rest of the home page.

Using def.xml for Custom Reports

The following example illustrates how the def.xml can be used up for creating your own custom reports.

To use this sample file, rename the def.xml.sample located at:

```
C:\Program Files\Opware\DCI\wwwroot\reports\custom\sample
```

to the name def.xml. Then, move the new file to this directory:

```
C:\Program Files\Opware\DCI\wwwroot\reports\custom\
```

for actual use and place in the appropriate directory or directories as described below.

What is a def.xml file?

The def.xml file is used to configure DCI reports for display in the OCC. When configuring the Custom Reports category of DCI, a def.xml file is typically created in the following directory:

```
C:\Program Files\Opware\DCI\wwwroot\reports\custom
```

directory to customize the display of the Custom Reports category in the OCC. Additional def.xml files may be created in subdirectories of:

```
...\wwwroot\reports\custom
```

to configure subfolders within the Custom Reports category. See file configuration details below for more information.

Layout of the def.xml file

The root element is the <sections> tag. Inside the <sections> tag are three types of sections:

- <text_section>: This is an optional section that can be used to display textual information on the page. Multiple text sections may be defined for a page.
- <folder_section>: This section is used solely in reporting category definitions to define subfolders within the category.
- <report_section>: This section is used to define report sections with report links and descriptions. Multiple text sections may be defined for a page.

When sections are displayed in the OCC, they are shown in the order in which they are defined in the def.xml file.

Sometimes you need to include data in this file that might contain XML-like tags and other data that you do not want XML to interpret. XML has a special section called CDATA that you can use to enclose text data. A CDATA section starts with

```
'<![CDATA['
```

and ends with

```
']]>'
```

You might, for example, want to include HTML text in the description for a text_section. You don't want the XML parser to interpret the HTML tags. Here is an example:

```
<description>
<![CDATA [
<b>This text appears in bold because the HTML tags are not
parsed by the XML parser</b>
]]>
</description>
```

Backup and Restoration of Custom Reports

When the DCI application is uninstalled from a server, the entire custom reports folder tree:

```
DCI\wwwroot\reports\custom
```

and below is copied to

```
DCI\CustomReportsBackup
```

If the DCI version 1.5 or later is then reinstalled to the same server, that folder tree will be restored to its proper location so that the custom reports will automatically be available just as they were previously. Custom reports that have been placed in any location other than DCI\wwwroot\reports\custom will not be backed up during uninstallation.

Sample def.xml file

```
-->
<sections>
  <!-- title is displayed by the DCI UI Navigation Display at top of
the page. This is not used if within a subfolder of a category that has
already defined the subfolder's displayname. -->
  <title>Custom Reports</title>
  <!-- The text section is an optional section used to display textual
information. -->
  <text_section>
    <!-- The title of the section -->
```

```
<title>Overview</title>
<!-- The descriptive content of the section. May include HTML if
enclosed in CDATA tags. -->
<description> The custom category is where the customer can add
their own folders and reports.
</description>
</text_section>
<!-- The folder section is used to display subfolders within a
reporting category. This section should only be defined in the def.xml
of a reporting category. It does not have any purpose
in the def.xml of a category subfolder. -->
<folder_section>
  <!-- title of section -->
  <title>My Folders</title>
  <!-- The folder section has a folder element for each subfolder
within the category. Folders are displayed in alphabetical order. -->
  <folder>
    <!-- The name of the physical subdirectory to which the
subfolder applies (required).
In this example, the subdirectory referenced by
'folder1' would be DCI\wwwroot\reports\custom\folder1 -->
    <name>folder1</name>
    <!-- The name to display in place of physical folder name
(if this element is not defined then the name value will be used for
displayname) -->
    <displayname>
      Sample Folder 1
    </displayname>
  </folder>
  <folder>
    <name>folder2</name>
    <displayname>
      Sample Folder 2
    </displayname>
  </folder>
</folder_section>

<!-- The report section is used to define links to reports. Multiple
report sections may be defined to group reports within the same page. -
-->
<report_section>
  <!-- The displayed title of the section -->
  <title>My Reports</title>
  <!-- One or more report elements should be defined for each
report section. Reports within the same report section are listed in
alphabetical order. -->
  <report>
    <!-- The report file name (required). If displayname is not
defined, this value will be used with the extension stripped off.-->
    <name>sample_report_1.rpt</name>
```

```

        <!-- The displayed report name (optional). If this element
is not defined then the name value will be used for display. -->
        <displayname>Sample Report 1</displayname>
        <!-- The description is displayed beside the report name
(optional) -->
        <description>... Description for report 1 ...</description>
        <!-- If the report is in the same folder as this file
(def.xml), leave PATH blank. If the report is elsewhere, enter the
location of the report relative to DCI/www/reports.
(For example, if the report is in
DCI\wwwroot\reports\custom\shared, enter
        custom\shared for PATH.) -->
        <path>custom\shared</path>
        <!-- An optional URL to the ASP used to display the report.
The URL may contain a query string. The parameter 'ReportName' is
always appended to the end of this URL as in '&ReportName=sample_
report_1.rpt'. The URL string should always be enclosed in CDATA tags.
-->
        <url>
            <![CDATA[
                viewer/
MyDCIViewer.asp?serverType=managed&FilterBy=Hostname
            ]]>
        </url>
    </report>
    <report>
        <name>sample_report_2.rpt</name>
        <displayname>Sample Report 2</displayname>
        <description>... Description for report 2 ...</description>
    </report>
</report_section>
</sections>

```

Chapter 5: DCI Report Server FAQ

IN THIS CHAPTER

This chapter discusses the following topics:

- How Do I Restart or Stop the DCI Report Server?
- How Do I Change the DCI Username and/or Password?
- How Do I Change the Public Views Password in Oracle?
- How Do I Change the Public Views Password In DCI?
- How Do I Keep the Public Views Password Secure?
- What Time Zone is Used in Reporting?
- Can I Share the DCI Report Server With Other Web Applications?

How Do I Restart or Stop the DCI Report Server?

In order to start and stop the DCI Report Server, perform the following steps:

- 1** On the DCI server, open the Crystal Configuration Manager from Programs ► Crystal Enterprise 10.
- 2** Right-click the Crystal Report Application Server (RAS) and select **Stop** to stop the RAS service.
- 3** Right-click the Crystal Report Application Server (RAS) and select **Start**.

How Do I Change the DCI Username and/or Password?

If you want to change the DCI user name and/or password, modify the following custom attribute values the server, and then use the DCI reconfigure control to implement the changes:

- `dci_admin_user`
- `dci_admin_pwd`

- 1** Find the server that hosts the DCI Report Server, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2** Select the server link (the server's name).
- 3** In the server's property page, select the Custom Attributes tab.
- 4** In the custom attribute list, scroll down and modify the values of the following attributes to create a new DCI user name and password:

`dci_admin_user`
`dci_admin_pwd`
- 5** Click **Save**.
- 6** To find the DCI Report Server you just added the new custom attribute to, search by name or IP address from Servers ► Manage Servers, or by Server Search
- 7** Select the check box next to the server (do not click the server name link).
- 8** From the **Tasks** menu, choose **Run ► Control**.
- 9** In the DCI Control dialog box, click the View Parameters link.
- 10** From the Application drop down list, make sure you choose dci-1.6 (Server) and that the Action drop down list is set to Reconfigure.
- 11** After you have make the appropriate changes to the attributes, click **Run**.



When you run the DCI reconfigure control, Apache server will be restarted and any users logged into the OCC at the time will be logged off.

How Do I Change the Public Views Password in Oracle?

If you have access permissions to the Oracle installation for Opware SAS, you can use SQL to change the Opware public views password (you must know the current password). After you have changed the Oracle password, you will have to change the password stored on the DCI Report Server. For information on changing the DCI Report Server password, see "How Do I Change the Public Views Password In DCI?" on page 75.

Perform the following steps to change the password in Oracle. For this example, we assume that the name of the new password will be "publicpassword".

- 1 Log in as root to the server where Oracle is running.
- 2 Bring up a terminal window and press return after each of the following steps
- 3 At the Unix command line type:

```
su - oracle  
and press ENTER.
```

- 4 Connect to Oracle through SQL*Plus by running:

```
sqlplus "/ as sysdba"
```

- 5 At the SQL> command-prompt type:

```
ALTER USER opsware_public_views IDENTIFIED BY  
publicpassword;  
and press ENTER.
```

- 6 You should see the message "User altered" which indicates the command ran successfully.
- 7 Exit SQL*plus by entering `exit` at the command line.

How Do I Change the Public Views Password In DCI?

The Public Views user ID is created on the DCI Report Server during installation and is used for authentication between the OCC and the DCI Report Server. To change the password value of Public Views password, modify the server custom attribute named `public_views_pwd` and then use the DCI reconfigure control to implement the changes.

- 1 Find the server that hosts the DCI Report Server, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2 In the server's property page, select the Custom Attributes tab.
- 3 In the custom attribute list, scroll down and modify the values of the following attributes to create a new DCI user name and password:

```
public_views_pwd
```

- 4 Click **Save**.
- 5 To find the DCI Report Server you just added the new custom attribute to, search by name or IP address from Servers ► Manage Servers, or by Server Search

- 6** Select the check box next to the server (do not click the server name link).
- 7** From the **Tasks** menu, choose **Run ► Control**.
- 8** In the DCI Control dialog box, click the View Parameters link.
- 9** From the Application drop down list, make sure you choose dci-1.6 (Server) and that the Action drop down list is set to Reconfigure.
- 10** Click **Run**.

How Do I Keep the Public Views Password Secure?

The DCI Report Server public views password is a custom attribute in the Opware Command Center. It is saved in plain text so the report server installer will configure the correct files to access the database for gathering report data. If keeping the password in this field in the Opware Command Center is a security issue, you can remove the value after you complete the installation. The `opware_public_views` user is a read-only account, and administrators with permission to view this server are able to see the value. You will need to set the password custom attribute again if you upgrade the server or set up a new DCI Report Server.

To make the DCI Report Server public views password secure, modify the DCI custom attribute named `public_views_pwd` so that its value is blank and then save the change. Do not reconfigure the DCI Report Server. (This assumes that you have already set the public views password at least once.)

To keep the DCI Report Server public views password secure, perform the following steps:

- 1** From the Opware Command Center, click Other Applications, then navigate to the DCI ► en ► 1.6 ► Windows 200<?> ► DCI 1.6.
- 2** Select the Custom Attributes tab.
- 3** Click the **Edit** button.
- 4** In the Custom Attributes page DCI server, locate the custom attribute named `public_views_pwd` and delete the value.
- 5** Click **Save**.

What Time Zone is Used in Reporting?

The core for an Opware SAS installation depends on UTC (Greenwich mean time). Thus, all reports display date and time information in UTC. This setting is not configurable. However, reports will show a time stamp from the DCI Server where IIS is installed.

Can I Share the DCI Report Server With Other Web Applications?

Yes, DCI Report Server is installed into its own work area within IIS on the server and should not interfere with other Web services that are running on the same servers.

Chapter 6: Troubleshooting DCI Report Server

IN THIS CHAPTER

This chapter discusses the following topics:

- Troubleshooting General Errors In the DCI Report Server
- Miscellaneous DCI Report Server Troubleshooting
- Contacting Opsware Support

Troubleshooting General Errors In the DCI Report Server

This section describes how to troubleshoot common DCI Report Server issues. If you are experiencing problems with your DCI Report Server, browse through these steps and determine if any apply to your situation.

- Step 1 - Did the DCI Package Upload?
- Step 2 - Did the DCI Report Server Install?
- Step 3 - Can You Access DCI in the OCC?
- Step 4 - Can You View a Standard Report?
- Step 5 - Do You See Any Custom Reports, And Are They Working?

Step 1 - Did the DCI Package Upload?

Check to make sure that the DCI package properly uploaded into the Opsware Command Center. If you experience problems with the upload process, contact Opsware Support. For more information on how to contact Opsware Support, see “Contacting Opsware Support” on page 88.

Step 2 - Did the DCI Report Server Install?

Verify that the DCI report server installed successfully by pointing to the server's URL from a Web browser (for example http://<server_name>/dci).

If DCI did not install properly, check the log files to see what error message was recorded. Errors that occur during installation are recorded in the Program Files\DCIPackage_en-1.6\logs\dcinstall.log file. You can also access this log file from the My Jobs details in the Opware Command Center. In addition to the log file, DCI also reports the following error codes to the Install Software Wizard, as shown in Table 6-1.

Table 6-1: DCI Report Server Installation Errors and Solutions

DCI INSTALLATION ERROR NUMBER/ DESCRIPTION	EXPLANATION/SOLUTION
<p>Error 100</p> <p>Insufficient disk space available. Installation halted.</p>	<p>The amount of space required for unpacking and installing the application components is not available. To solve this problem, uninstall the DCI Report Server software, ensure the documented space requirements are met, and begin installation again.</p>
<p>Error 101</p> <p>IIS has not been installed or started.</p>	<p>Check IIS prerequisites. This means that the IIS service is not running. Ensure that IIS is installed and running, then uninstall the DCI Report Server and begin installation again.</p>
<p>Error 102</p> <p>RAS installation failed.</p>	<p>Check the Event Viewer. The Report Application Server installation failed. Check the Event Viewer for any relevant errors. Uninstall and begin installation again.</p>
<p>Error 103</p> <p>Failed to create the Virtual Directory DCI.</p>	<p>Check the Event Viewer. The installation could not create the IIS virtual directory, possibly due to inappropriate custom attribute settings. Check the log for explanatory messages, resolve any issues, and run the dci-1.6 reconfigure control (Managed Servers > Tasks > Control).</p>
<p>Error 113</p> <p>Failed to enable ASP Scripting in IIS 6.0.</p>	<p>IIS could not be configured to allow ASP scripting. Check the log for explanatory messages, resolve the issue, uninstall and begin installation again.</p>
<p>Error 114</p> <p>DCI requires Service Pack Level 3 or higher for Windows 2000.</p>	<p>Windows 2000 appears to be at an unsupported Service Pack level. Ensure that Service Pack 3 or later is installed, uninstall and begin installation again.</p>

Table 6-1: DCI Report Server Installation Errors and Solutions

DCI INSTALLATION ERROR NUMBER/ DESCRIPTION	EXPLANATION/SOLUTION
Error 115 Failed to install ODBC Drivers (%errorlevel%).	The ODBC Driver installation failed. Uninstall and begin installation again.
Error 118 DCI currently installed.	Please follow upgrade procedures. Then Check IIS prerequisites. The DCI Report Server application appears to already exist on the server. Ensure that this is not the case. This is triggered by the presence of the directory %Program Files%\Opware\DCI\wwwroot\common. If this directory has been left behind after an uninstall, remove it, uninstall, and begin installation again.
Error 119 Failed to contact (ping) the Data Repository, truth.host (%truthhost%).	The hostname "truth" must be accessible from the DCI server. Verify connectivity and name resolution, uninstall, and begin installation again.
Error 122 Failed to contact (ping) the NAS Database Host, (%nas_db_host%).	The IP address/hostname provided could not be accessed from the DCI server. Verify the address or hostname, and connectivity, then uninstall and begin installation again.
Error 131 Incomplete NAS configuration.	You must supply all parameters or none. The five custom attributes for NAS reporting must either all be blank, or contain all values. Uninstall the package, set the appropriate values as described in the documentation and begin the installation again.
Error 132 Failed to contact (ping) the OCC host (%occ_ip%).	The IP address provided could not be accessed from the DCI Report Server. Verify the address and connectivity, uninstall and begin installation again.
Error 139 Invalid argument: '%1'.	Must be either install or reconfig. The installation/reconfiguration was not started through the OCC's install/control interface. Contact Opware Customer Support.

Table 6-1: DCI Report Server Installation Errors and Solutions

DCI INSTALLATION ERROR NUMBER/ DESCRIPTION	EXPLANATION/SOLUTION
Error 140 Failed to retrieve custom attributes from ISM parameters interface.	The ISM could not access the custom attributes. Contact Opware Customer Support.
Error 141 Missing one or more required Custom Attributes.	All five of the custom attributes related to SAS reporting are required. Uninstall the package, set the appropriate values as described in the documentation and begin installation again.
Error 138 Failed to configure OCC for DCI access. Configuration of the OCC failed.	Possibly due to inappropriate custom attributes. Correct the custom attribute values, and run the dci-1.6 reconfigure control (Managed Servers ► Tasks ► Control).
Error 255 Failed to create DCI Admin User. Could not create the DCI Admin User account.	Possibly due to inappropriate custom attribute settings. Check the log for explanatory messages, resolve any issues, and run the dci-1.6 reconfigure control (Managed Servers ► Tasks ► Control).

Step 3 - Can You Access DCI in the OCC?

If your DCI Report Server was installed and configured correctly, you should be able to access it from the OCC. You will know if the installation and configuration was successful if you can see the following DCI links in the OCC:

- The View Reports in the Power Tools section of the OCC home page.
- The View Reports link in the navigation panel
- A list of links below the Report links in the navigation panel: Server Reports, Compliance Center, Network (if you have NAS configured), Custom Reports, and Ad Hoc Reporting

If you do not see the DCI Report Server links in the OCC, try the following steps:

- 1 Inside the OCC where your DCI Report Server is installed, from the navigation bar click the Configuration link to go to the System Configuration page.

- 2** On this page, click the Opsware Command Center link.
- 3** Scroll down the page and double check the parameter named `owm.features.Reports.allow` has its value set to `true`. True means the installation was successful. If the value is set to `false`, there was a problem with the installation and you will need to troubleshoot the error. If you see a `true` value, click **Save** at the bottom of the page. Even if you make no changes, click **Save** to ensure the proper configuration. You should now see the Reports link in the navigation panel.

If you are viewing a DCI Report Server in a multimaster mesh where there might be more than one DCI Report Server, make sure that you modify the correct DCI Server in the mesh.

Step 4 - Can You View a Standard Report?

If you can view the DCI home page but can not click on a report name to view an actual report, several problems might be occurring. The following error is caused by having cookies in your browser turned off.

* Error Type:

```
Microsoft VBScript runtime (0x800A01A8)
Object required: 'Session(...)'
```

To fix this problem in Internet Explorer 5.x and 6.x, go to Tools ► Internet Options ► Privacy and move the security slider for cookies to medium or lower. If you are receiving a different VBScript runtime error, it might be caused by insufficient memory on the report server. Try increasing the server's memory. If the runtime error still persists, send the error details to Opsware support for assistance.

If you see an ODBC login screen, it is possible that your database connection is not properly configured. Check to make sure that:

- For SAS reports, the following custom attributes must be configured correctly:

```
public_views_pwd
sas_db_sid
```

- For NAS reports, all custom attributes must be configured correctly.

To set custom attributes to the DCI Report Server software node, perform the following steps:

- 1** Find the server that hosts the DCI Report Server, by name or IP address from Servers ► Manage Servers, or by Server Search.
- 2** Select the check box next to the server (do not click the server name link).
- 3** From the **Tasks** menu, choose **Run ► Control**.
- 4** In the DCI Control dialog box, click the View Parameters link.
- 5** In the custom attribute list, scroll down and modify the values of the appropriate custom attributes.
- 6** After you have make the appropriate changes to the attributes, click **Run**.

Step 5 - Do You See Any Custom Reports, And Are They Working?

If you can view a standard report, but not a custom report, the problem lies within either your custom report itself or the custom configuration definition file (def.xml).

First, check to make sure your custom reports reside in the proper folder. Then, check to make sure the custom configuration properties file has been properly written. See Chapter 5, "DCI Report Server FAQ" on page 73 of this guide for more information.

Miscellaneous DCI Report Server Troubleshooting

This section shows you how to solve various problems you might encounter with DCI Report Server and contains the following topics:

- Delay Occurs While Generating Some Server Reports
- Prompt for User Name/Password When Accessing DCI Home Page
- Database Login is Displayed When Running a Report
- Microsoft VBScript Runtime Error
- Running a Report Returns a Page Full of "unspecified errors"
- Images and Graphs Missing on a Report
- A Report "hangs" for Longer Than Five Minutes
- Troubleshooting Windows Permissions for DCI

- DCI User Not Created on Windows
- Error Seen on All Links in a Report

Delay Occurs While Generating Some Server Reports

If you experience a delay in the generation of some server reports, there are two factors that could produce this delay: one is a delay in database updates as result of reconcile processes; the other is related to the caching of report data by Crystal RAS.

Crystal RAS has a configuration setting for the maximum time that previously queried data is allowed to be displayed in a report before refreshing the data. The default setting is one hour. Reports will display faster as long as cached data is used. Increasing this value causes data to be cached longer. Once the cache expires, the report has to requery the data, which will slow the report by the amount of query time. Reducing the setting causes the data to be cached for a shorter period of time and allows changes in Opware SAS to be seen in reports sooner.

To modify the RAS data caching, perform the following steps:

- 1** On the DCI server, open the Crystal Configuration Manager from Programs/Crystal Enterprise 10.
- 2** Right click the Crystal Report Application Server (RAS) and select **Stop**.
- 3** Right-click again and choose **Properties** to display the Properties page.
- 4** Select the Parameters tab to display the RAS parameter settings.
- 5** Change the Data Refresh setting to the maximum allowable age of cached report data in minutes. This value may be set to zero to always retrieve the most recent data.
- 6** Right-click the Crystal Report Application Server (RAS) and select **Start** to start the RAS service.

Prompt for User Name/Password When Accessing DCI Home Page

If you attempt to access the DCI Report Server and you are prompted with a pop up dialog asking for a user name and password, it is possible that the `dci_admin_user` and `dci_admin_pwd` are not properly configured. For information on how to set these custom attribute values, see the instructions for changing DCI Report Server custom attributes in the troubleshooting step named "Step 4 - Can You View a Standard Report?" on page 83.

Database Login is Displayed When Running a Report

This probably means that the Crystal Reports Application server in the DCI Report Server is unable to connect to the database. There are several possible solutions:

- Check that the Opware DCI ODBC configuration is valid.
- Check that the host, port, and SID settings are correct. For more information, see the troubleshooting step named “Step 4 - Can You View a Standard Report?” on page 83.
- Verify that the host is accessible from the DCI Server. For SAS reports, the hostname “truth” should be assessable. For NAS reporting, the custom attribute named nas_db_host must be correct.
- Verify that the database and its listener are started.

Microsoft VBScript Runtime Error

If you run a report and get the following error:

```
Microsoft VBScript runtime error '800a01a8' Object required:
'Session(...)'
```

This means that the ASP within the DCI Web application redirects the request to another URL and the browser is unable to obtain the session cookie for the current ASP session. Ensure that the browser is configured to accept cookies.

Running a Report Returns a Page Full of “unspecified errors”

In some cases, running a report may result in a page full of errors beginning with:

```
Unspecified error; Error code 0x80004500; Source:
webReporting.dll.
```

Error messages will also include:

```
renderPage failed
```

and

```
RenderContent failed
```

Typically this error is seen when either the dciadmin user or the IUSR_<machinename> user on the DCI server do not have appropriate permissions to the system TEMP directory. Grant full access to the system TEMP directory and its subdirectories. If this does not correct the problem, see “Troubleshooting Windows Permissions for DCI” on page 87.

Images and Graphs Missing on a Report

Typically this error is seen when the IUSR_<machinename> user on the DCI server does not have appropriate permissions to the system TEMP directory. Grant full access to the system TEMP directory and its subdirectories. If this does not correct the problem, see “Troubleshooting Windows Permissions for DCI” on page 87.

A Report “hangs” for Longer Than Five Minutes

A report can appear to be hanging for the following reasons:

- The report is running, yet it is either very complex or has to process a large amount of data or both. Some reports can run for hours in an environment with a large amount of data.
- The report is running, yet there are problems with database optimization.
- The number of available Crystal Report sessions has been exceeded and the current report is waiting for one to become free. The default number of session licenses is three. This becomes a problem when the number of reports being run exceeds the number of session licenses. Licenses should be increased if report usage warrants it.
- There may be a problem with either IIS or the Crystal Reports Application Server. Restart IIS and then restart the Crystal Report Application Server service.

Troubleshooting Windows Permissions for DCI

In general, when there are potential permission problems in Windows, use the following procedure to pinpoint the issues:

- Use the Windows Local Security Policy tool to set the local Audit Policy to audit failed object access attempts.
- Go to Properties of the C: root directory, click the Advanced button on the Security tab, then set Auditing on the Users group to Full Control for Failed access. After clicking OK, it may take a while to propagate the settings to all subdirectories. You could set up Auditing on more specific directories, but this approach ensures that we catch all access problems on C:. Of course, these settings should all be temporary until the problem is resolved.
- Reproduce the permissions-related error and check the Security event log for failed access events. Events of type 560 should specify the user, the object being accessed, and the requested permissions.

DCI User Not Created on Windows

If the password that you specify in `dci_admin_pwd` does not meet the security requirements for the DCI Report Server, then the DCI user will not get created. If this is the case, you will see installation error 255. For more information on this installation report error, see “Step 2 - Did the DCI Report Server Install?” on page 79.

To fix this problem, you will need to reset the `dci_admin_pwd` with a value that meets the security requirement of your facility. For information on how to change this password, see the instructions for changing DCI Report Server custom attributes in the troubleshooting step named “Step 4 - Can You View a Standard Report?” on page 83.

Error Seen on All Links in a Report

The DCI home page loads but all links have the following error

```
* Error Type:
  clientdoc.dll (0x80041015)
  Failed to connect to server "<servername>". Error
  returned from Windows Sockets API : 0.
  /DCI/viewer/customReportViewer.asp, line 29
```

To solve this problem, restart Crystal Reports.

Contacting Opware Support

When you contact Opware Support, have the following information available to help you with your support call:

- Be at your computer and have network access to the servers running the Opware core.
- Have your Opware guides available.
- Write down the steps followed prior to the problem occurring.
- Write down the exact text of the error appearing on your screen or print out the page on which the error appears.
- Be able to describe the problem in detail.

Contact Opware Technical Support:

Phone: +1 877 677-9273 (1-877-Opware), in the United States

International Phone: 1 408-212-5300

E-Mail: support@opware.com

Index

C

- changing
 - DCI admin password 73
- contact Opsware Support 88
- contacting, Opsware viii
- conventions used in the guide vi
- custom reports
 - extending reports with other data sources 66
 - installing 67
 - not working, what to do 84
 - understanding access to public views 65
 - using shipped report to create a custom report . 65

D

- DCI
 - homepage does not appear, what to do 82
 - package did not upload, what to do 79
- DCI Report Server
 - did not install, what to do 79
 - installing
 - using ISMTool 5
 - starting/stopping 73
 - time zone used in reporting 77
- DCI Report Server FAQ 73

E

- extending reports with other data sources 66

I

- installation prerequisites 1
- installing
 - a customized report 67
 - the DCI Report Server
 - using the ISMTool
 - overview 5

K

- keeping public views password secure 76

O

- Opsware guides
 - contents of v
 - conventions used vi
 - documentation set vii
 - icons in guide, explained vi
- Opsware SAS
 - documentation set vii
 - related documentation vii
- Opsware Support, contact 88

P

- password
 - changing for DCI admin 73
 - changing for Oracle public views 74
 - keeping secure for public views 76
- prerequisites for installation 1

R

- restarting/stopping the DCI Report Server 73

T

- time zone used in reporting 77

U

- understanding access to public views 65
- using a shipped report to create a custom report . 65

