

Oracle® DIVAdirector

Administrator's Guide

Release 5.4.1

E86633-03

February 2018

Oracle DIVAdirector Administrator's Guide, Release 5.4.1

E86633-03

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	vii
Conventions	vii
1 Introduction	
Preparing for Installation	1-1
Supported Proxy and Audio Formats	1-2
2 Initial DIVAdirector Configuration	
Changing the Administrative Password	2-1
Confirm Oracle DIVA Enterprise Connect Connectivity	2-1
Configuring DIVAdirector User Interface	2-3
System Settings	2-3
Default Settings	2-3
DIVArchive Settings	2-4
Connections	2-5
Housekeeper File Management Settings	2-5
Database Pre-caching Settings	2-5
System Synchronization	2-6
Manual Synchronization	2-6
Synchronization Maintenance	2-7
Synchronization Filtering	2-7
Configuring Keyboard Shortcuts	2-7
Shotlist Shortcuts	2-9
Proxy Player Shortcuts	2-9
Style	2-9
Configuring DIVAdirector Web Server	2-9
Listening Port Configuration	2-10
IIS Service Account Configuration	2-10
Account Configuration	2-10
Adding an Organization	2-10
Adding a Group	2-11
Group Roles	2-12

General Privileges	2-12
DIVArchive Operation Privileges.....	2-13
Administration Privileges.....	2-14
System Administration Privileges	2-14
Content Filters	2-15
Metadata Permissions	2-16
DIVArchive Operations	2-16
Data Export	2-18
Source/Destination Configuration.....	2-18
Adding a User.....	2-18
Drop Folder Configuration.....	2-19
DIVArchive Operation Drop Folders.....	2-22
Annotation Drop Folders	2-25
Adding Proxy Drop Folders	2-26
Map the Storage Location in Windows and Set Folder Permissions.....	2-26
Add the Proxy Folder to the DIVAdirector Web Server in IIS.....	2-27
Configuring the Proxy Storage Location	2-27
Add Proxy Drop Folder	2-28
Proxy Drop Folder File Format	2-28
Proxy Generation.....	2-29
Adding Category Filters.....	2-29
DIVArchive Restore Options.....	2-30
Scheduling.....	2-30
Proxy Migration.....	2-30
Transcode Service Configuration.....	2-31
Starting and Stopping the Transcode Service Windows Services.....	2-32
Configuration File Changes.....	2-32
Vantage Implementation.....	2-35
Vantage Stand-alone Integration.....	2-35
Configuring the Vantage Stand-alone Presets	2-35
Configuring Vantage Split Workflow	2-36
Multiple Transcoders and Load Balancing	2-38
Command Line Transcoder - Custom Script Integration.....	2-38
Configuring the Command Line Transcoder Script	2-38
Custom Script Parameters	2-39
Logging Configuration.....	2-40
Oracle DIVAdirector WWW Logging Configuration.....	2-41
Oracle DIVAdirector Task Manager Logging Configuration.....	2-42
Oracle DIVAdirector API Logging Configuration	2-42
Search Configuration.....	2-42
Object Metadata.....	2-42
Data Types	2-43
DIVAdirector Presentation Controls.....	2-43
Predefined Metadata Display Columns	2-44
Adding a Metadata Entry	2-45
Add Quality Control Metadata	2-46
Metadata Filters.....	2-47

Metadata Publish Settings.....	2-47
Automated Backup Configuration	2-47
Quality Control (QC) Report Configuration	2-48
QC Report File Placement.....	2-48

3 DIVAdirector Daily Operations

Checking Available Storage Capacity.....	3-1
Checking for Orphaned Files.....	3-2
Checking Audit Trails.....	3-2
Checking for Successful Backup Completion.....	3-3

4 System Management

Database Synchronization Management.....	4-1
Proxy Storage Management.....	4-2
User Data and Resource Management.....	4-2
Making a Public Resource Private.....	4-2
Account Management.....	4-2
Managing Organizations.....	4-3
Modifying an Existing Organization.....	4-3
Deleting an Organization.....	4-3
Managing Groups.....	4-3
Modifying an Existing Group.....	4-3
Deleting an Existing Group.....	4-3
Managing User Accounts.....	4-4
Modifying an Existing User.....	4-4
Deleting a User.....	4-4
Search Management.....	4-5
Metadata Column Manager.....	4-5
Editing a Metadata Entry.....	4-5
Deleting a Metadata Entry.....	4-5
Session Management.....	4-6
Administrator's Message.....	4-6
Configuration for ShuttlePro V2 or ShuttleXpress Control Pads.....	4-6

5 Troubleshooting and Disaster Recovery

Task Manager and DIVAdirector API Windows Services.....	5-1
Task Manager Service.....	5-1
DIVAdirector API Service.....	5-2
Starting and Stopping the DIVAdirector Web Server.....	5-2
Checking Log Files.....	5-2
Manual Backup and Database Restore.....	5-3
Performing a Manual Backup.....	5-3
Performing a Database Restore.....	5-3

6 Frequently Asked Questions

Glossary

Preface

This document gives a basic understanding of system functionality and detailed instructions for configuring Oracle DIVAdirector 5.4.

Audience

This document guides System Administrators through initial Oracle DIVAdirector system configuration, daily operations, and routine maintenance.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see the Oracle DIVAdirector documentation set for this release located at <https://docs.oracle.com/en/storage/#csm>.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements that perform an action.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Introduction

Oracle DIVAdirector is a graphical user interface (GUI) for Oracle DIVArchive 7.4 and later. Through the web interface you can locate and work with videos remotely, from any computer on your network. Administrators monitor and maintain the system and user accounts with minimal effort from anywhere they have access to your network.

You access DIVAdirector through a web browser using the HTTPS protocol. Some of the advantages of a web-based interface include:

- No GUI software installation is required.
- A browser-based GUI can be accessed from anywhere on the network.
- No client application configuration is necessary.
- No client updates are required.

Using DIVAdirector you can:

- Search for video clips by file name, date, category, and format.
- Define metadata fields that support search.
- Use advanced search operations to hone searches for specific criteria. For example you can search for video clips of farm animals in the United States, but not in Nebraska or Kansas.
- Review located clips using the built-in media player.
- Extract selected frames, add them to a list of related clips, forward them to editing applications, or arrange them for distribution.

Note: DIVAdirector 5.4 and later is licensed per user, not per concurrent user. You identify the maximum concurrent users (between 1 and 100) on the **Admin, System, Defaults** screen.

Preparing for Installation

Before the Oracle Delivery and Installation Team arrives at your site you must complete installation and configuration of your system hardware. See the *Oracle DIVAdirector Installation Guide* in the *Oracle DIVAdirector documentation* library for details on preparing for installation.

You must have at least one fully operational client computer available for testing during and after installation. Client computers must have Microsoft Windows 7 Professional or Ultimate (either 32-bit or 64-bit) with Service Pack 1, or macOS 10.6 (Snow Leopard) or later, operating system installed, and one of the following supported web browsers:

- Internet Explorer 11 or later
- Microsoft Edge for Windows 10
- Chrome 45 or later
- Firefox 38 or later
- Safari 8.0 or later

Note: Playback of WMV files are only supported in Internet Explorer with the Silverlight plug-in installed.

Supported Proxy and Audio Formats

More recent browser releases (in general) no longer support NPAPI applications such as Silverlight and QuickTime. This is a browser limitation, not a DIVAdirector limitation. Oracle recommends using MP4 as the standard video format.

DIVAdirector 5.4 and later supports the following proxy and audio formats. *DIVAdirector 5.4 does not currently support discontinuous timecodes.*

MP4 (recommended)

- Container: MP4 with MOOV atom at beginning of file (fast start)
- Video Codecs: Mpeg-4 Part 10 (H.264)
- Video Frame Rates: 24 fps, 25 fps, 29.97 fps are verified.

The frame rate should be as close to the source rate as possible. Oracle recommends maintaining the aspect ratio, but you can adjust the exact frame size based on any limitations of your system.

- Video Bitrates: 400 Kbps to 5000 Kbps

The optimum bitrate will depend on available bandwidth and other video settings (frame rate, resolution, and so on).

- Audio Codecs: AAC
- Audio Bitrates: 128 Kbps
- Audio Sampling Rates: 44.1 kHz

MP3 (recommended)

- Container: MP3
- Audio Codecs: MP3
- Audio Bitrates: 128 Kbps
- Audio Sampling Rates: 44.1 kHz

Silverlight

- Container: WMV
- Video Codecs: WMV1, WMV2, WMV3, VC-1
- Video Bitrates: 100 to 1042 Kbps, constant

Note: Bitrates above 1042 Kbps can impact browser bandwidth and processing power. Oracle recommends using 1042 Kbps or lower bitrates.

- Audio Codecs: WMA
- Audio Bitrates: 32 Kbps, 48 Kbps, 512 Kbps, constant
- Audio Sampling Rates: 22kHz, 44kHz (44kHz is standard)

QuickTime

- Container: MOV
- Video Codecs: AVC
- Video Bitrates: 506 to 1042 Kbps, constant

Note: Bitrates above 1042 Kbps can impact browser bandwidth and processing power. Oracle recommends using 1042 Kbps or lower bitrates.

- Audio Codecs: AAC
- Audio Bitrates: 64 Kbps, 128 Kbps, constant
- Audio Sampling Rates: 22 kHz, 44 kHz (44 kHz is standard)

Initial DIVAdirector Configuration

You must continue to configure DIVAdirector after the Oracle Delivery and Installation Team has completed the initial installation. You typically complete the initial configuration tasks in this chapter one time unless there are major system or network changes (for example if IP addressing changes, port numbers change, and so on).

This chapter describes initial configuration after installation and includes the following information:

- Changing the Administrative Password
- Confirm Oracle DIVA Enterprise Connect Connectivity
- Configuring DIVAdirector User Interface
- Configuring DIVAdirector Web Server
- Account Configuration
- Source/Destination Configuration
- Proxy Generation
- Proxy Migration
- Transcode Service Configuration
- Logging Configuration
- Search Configuration
- Quality Control (QC) Report Configuration
- Automated Backup Configuration

Changing the Administrative Password

The installation technician installs DIVAdirector using a default administrative login and password, both of which are `admin` (these are case-sensitive and all lowercase). You will be prompted to change the DIVAdirector administrative password when you log in for the first time.

Confirm Oracle DIVA Enterprise Connect Connectivity

DIVAdirector interacts with DIVArchive using a standards-based Web Service API. The integration with this service, Oracle DIVA Enterprise Connect (DIVAEC), is configured in two different configuration files in DIVAdirector. Both of these files

should be configured automatically during the installation process. However, Oracle recommends manually verifying the configuration.

The first file is `web.config` located in the `www` folder in the installation directory (for example, `C:\Program Files (x86)\DIVAdirector 5\www\web.config`). The second file `Oracle.DIVAdirector.TaskManager.exe.config` located in the `TaskManager` subdirectory in the installation directory (`C:\Program Files (x86)\DIVAdirector 5\TaskManager\Oracle.DIVAdirector.TaskManager.exe.config`).

The following keys are duplicated in the `appSettings` section of both files:

DIVArchiveApiUrl

This key identifies the URL of the Oracle DIVA Enterprise Connect endpoint.

```
<add key="DIVArchiveApiUrl"
value="https://server:9444/diva/service/rest/2.2/DIVArchiveWS_REST" />
```

DWSVersion

This key identifies the version of the API Service DIVAdirector will target.

```
<add key="DWSVersion" value="2.2" />
```

ClientId

This key identifies the user name to connect to the API. This value is generated on the DIVA Enterprise Connect server.

```
<add key="ClientId" value="e3af4c10-e7ca-4143-970a-46bc0264a46f" />
```

ApiKey

This key identifies the password to connect to the API. This value is generated on the DIVA Enterprise Connect server.

```
<add key="ApiKey" value="kAkWTK3ObnEOmHheJAKP" />
```

AppName

This key identifies the name of the application invoking the services. This value is used when creating a client session.

```
<add key="AppName" value="DIVAdirector" />
```

ProcessId

This key identifies the ID of the client process that is executing, or another unique ID that identifies the instance of the application that is executing. This value is used when creating a client session.

```
<add key="ProcessId" value="1234" />
```

LocationName

This key identifies a string describing the location of the client (caller). This value is used when creating a client session.

```
<add key="LocationName" value="DIVAdirector Web" />
```

Use the following procedure to confirm that Oracle DIVA Enterprise Connect is operational:

1. Open a Web Browser from the DIVAdirector Server.

2. Navigate to `http://server:7001/ws_utc/login.do`.
3. If you are able to log in to the *Try It* interface, then the service is operational. Otherwise, consult the Oracle DIVA Enterprise Connect documentation to resolve any issues with the service.

Configuring DIVAdirector User Interface

Now that you have configured all of the network and system connectivity, you must configure the internal system parameters that affect how users interact with DIVAdirector and DIVArchive. To configure the DIVAdirector user interface navigate to the **Admin, System** menu tree on the left side of the GUI screen.

First you will configure the System Settings.

System Settings

The *Defaults* screen enables configuration of systemwide default values. For example, the language that search metadata is collated in, the global date and time display format, and so on.

1. Navigate to the *Defaults* screen under the **Admin, System** menu tree on the left side of the GUI.
2. Enter the appropriate values that are optimal for your organization and users for each option.

As the System Administrator you can identify most of these values according to existing organizational policies and your physical location. For example, calendar display format, time display format, and so on.

Default Settings

The following fields are configurable in the *Default Settings* area of the screen:

Search Language

Caution: Recalculating your search language is an exhaustive database procedure and should be completed only during a maintenance window of at least eight hours with the guidance of Oracle Support.

Defines the language used to optimize full text search. If your metadata is mainly not in a particular language, or your language is not in the list, then select the *Simple* option.

Default Query Result Sort Order

Defines a metadata column that is used as the primary source for sorting.

Date Display Format

Defines the format used for all date-type fields in DIVAdirector.

The list includes three format options.

- American - mm/dd/yyyy
- European - dd/mm/yyyy

- Custom - This option does not support any codes except *dd*, *mm*, *yy*, and *yyyy*. The order of the codes is arbitrary and can be whatever you define (can be defined in a relatively free-style format, for example *yyyy.dd.mm*). The allowed separator symbols are:
 - Space
 - Period
 - Comma
 - Underscore
 - Hyphen
 - Colon
 - Slash
 - Backslash

Time Display Format

Defines whether the time is displayed in 12 hour or 24 hour format.

Calendar Display Format

Defines the first day of the week in the calendar.

Max Metadata Label Length in Tooltip

Defines the maximum number of characters to display in the Tooltips label. If the metadata field title exceeds this setting it will be truncated with three dots at the end.

Max Metadata Field Length in Tooltip

Defines the maximum number of characters to display in Tooltips content. If the metadata field value exceeds this setting it will be truncated with three dots at the end.

Keyframe Extraction Workflow Name

Defines the transcoding workflow that handles frame extraction for shot list segments and annotations.

Rename Local Restore Downloads

Define a user defined metadata field to replace the name of downloaded files. The metadata field must be of the Text type and must have a length of 100 characters or less to be selectable.

Note: This option is only visible if enabled through the Web.Config file.

DIVArchive Settings

The following field is configurable in *DIVArchive Settings* area of the screen:

Rename Local Restore Downloads

Defines a user defined metadata field to replace the name of downloaded files. The metadata field must be of the Text type and must have a length of 100 characters or less to be selectable.

Note: This option is only visible if enabled through the Web.Config file.

Local Archive Base Path

This field is the physical path of the virtual directory that local archive files are being stored in. Generally this field is populated during installation, but you can modify it here if needed.

Connections

The following field is configurable in the *Connections* area of the screen:

External Domain Url

Defines the external url of the DIVAdirector server such that password recovery links and Oracle Client Uploader installers can be used from outside the network.

Maximum Number of Concurrent Users Allowed

DIVAdirector 5.3 and later licensing is per user, not per concurrent user. You set the maximum number of concurrent users (between 1 and 100) in this field. If no entry is made, the default number of users (100) is used. The maximum number of concurrent users is restricted by the amount of system resources available. If the system appears to slow down with a certain number of concurrent users online, you should lower the maximum number and reevaluate the performance.

Housekeeper File Management Settings

The following fields are configurable in the *Housekeeper File Management Settings* area of the screen located under **Admin, System, Service Settings, House Keeper**:

Local Request Files

Defines the number of days to keep the files that have been restored to the DIVAdirector Server host computer through all local request operations (Restore, Partial File Restore, Archive folders, and so on).

DIVArchive Request Status

Defines the number of days to keep the DIVArchive status information on the *Operation Status* screen.

Audit Trail

Defines the number of days to keep the audit trail and Drop Folder log information.

System Logs

Defines the retention policy for all DIVAdirector logs.

Scheduled Backups

Defines the number of days to keep backup files created by scheduled backups.

Database Pre-caching Settings

The following fields are configurable in *Database Pre-Caching Settings* area of the screen:

Current Memory Utilization

Displays the current memory use on the server.

Pre-Caching Selection

Defines which tables, if any, are to be held in memory for easy access. This can dramatically speed up certain functional areas of the application.

Next you will configure the System Synchronization.

System Synchronization

The *System Synchronization* page enables configuration of frequency and size of synchronization actions between DIVAdirector and DIVArchive. You can also observe synchronization tasks, downloadable logs for each task execution, set flags to permanently delete objects that no longer exist within the archive system, or delete proxies that have been removed on this screen.

1. Navigate to the **Synchronization** screen under the **Admin, System** navigation tree on the left side of the GUI.
2. You can adjust the frequency and size of each synchronization call under the *Automatic Synchronization* section on the top right of the screen.

Note: For systems that have numerous files per object, you should lower the *Objects Per Call* value. The lower value slows the rate of synchronization, while avoiding any potential request timeouts.

3. You can stop, or start, synchronization at any time by clicking **Stop/Start** above the Synchronization Tasks list. Stopping synchronization cancels any currently executing synchronization task.

Manual Synchronization

Caution: Synchronization processes are highly demanding and will result in some performance degradation until they are complete. You must only run manual synchronization operations during off hours, or at the request of Oracle Support.

You can perform a manual synchronization at any time. Performing a manual synchronization supersedes any active automatic synchronization currently processing. Automatic synchronization will resume after all manual tasks are complete.

There are three types of Manual Synchronization as follows:

Partial

A Partial Synchronization specifies that synchronization will occur from a given date forward. Only objects that were removed from the archive system within this period will be marked as inactive.

Full

A Full Synchronization will synchronize the entire contents of the archive system. A full synchronization initially marks all objects in a **Synchronizing** state. In this state they will still be searchable, but DIVArchive operations will not be allowed until they have been moved back to an **Active** state. Any objects that were not found during synchronization will be marked as **Inactive**. Inactive objects are not reflected in search results.

New Instance

Similar to Full Synchronization, this option will synchronize the entire contents of the archive system. This option assumes that large portions of the current synchronized objects are invalid and will initially mark all objects as **Inactive**.

Synchronization Maintenance

You can configure two housekeeping flags to cleanup synchronization artifacts as follows:

Delete Inactive Objects

This button notifies the housekeeper to permanently delete objects marked as **Inactive** by the synchronization process once per day. Proxies and binary files associated with deleted objects are moved to the `deleted` folder in their respective proxy storage location.

Delete Inactive Proxies

This button notifies the housekeeper to permanently delete all files contained within the `deleted` folders on each proxy storage location.

Synchronization Filtering

Synchronization filters define which objects are processed during synchronization. Each synchronization filter represents a combination of an object's parameters such as object name, object category and media name, and has its own *time of last synchronization*. Parameters can be defined as masks using the asterisk wildcard. By default the asterisk is set for fields that are empty. Filters with an asterisk in all three fields are invalid and cannot be added to the filter list.

All synchronization filters are inclusive of each other and are maintained by their own synchronization process. Because they are inclusive, the ordering of the filters does not matter.

You must issue a *New Instance* manual synchronization (as previously described) if you have added filters after DIVAdirector has already been synchronized and want to remove objects that do not conform to the new filters. This manual synchronization will mark all objects that were not found within these filters as **Inactive** and they can be removed during housekeeping.

Next you will configure the Keyboard Shortcuts.

Configuring Keyboard Shortcuts

Caution: You must be careful during configuration of keyboard shortcuts because they may coincide with hot keys used in internet browsers or other software, and cause unexpected results.

Keyboard shortcuts save time when performing common routine procedures during daily work tasks. DIVAdirector has hot key combinations that are predefined and configured automatically during installation.

The Proxy Player can be run in two different modes; *Shotlist Mode* and *Proxy Player Mode*. There are two corresponding subsections in the **Admin, System, Shortcuts** navigation tree - one for each mode. Each subsection defines the keyboard bindings for the player in that specific mode. You should assign keyboard shortcuts for the Proxy Player in each mode.

The following hot key combinations are predefined in DIVAdirector:

Control+e
Edit

Shift+1

Rewind x4

Shift+2

Rewind x8

Shift+3

Fast Forward x4

Shift+4

Fast Forward x8

Shift+a

Add

Shift+b

Frame Back

Shift+d

Decrease Volume

Shift+f

Forward

Shift+i

Mark In

Shift+l

Loop

Shift+m

Mute

Shift+n

Frame Forward

Shift+o

Mark Out

Shift+p

Play or Pause

Shift+r

Rewind

Shift+s

Stop

Shift+t

Switch Time Format

Shift+u

Increase Volume

Shift+x

Mark Out and Add

Use the following procedure to change the shortcut key combinations for either subsection:

1. Navigate to the **Admin, System, Shortcuts, Shotlist Shortcuts** screen, or to the **Admin, System, Shortcuts, Player Shortcuts** screen, as applicable.
2. Click the **Pencil** icon to edit the desired hot key combination.
3. Select the required combination of Control+ Shift {Key}. Where {Key} is the key to assign to the shortcut.
4. Click the **Check** mark to save the changes.
5. Test all of the configured hot keys, one at a time, to ensure there are no conflicts with other applications installed on the system.

Shotlist Shortcuts

You configure hot keys used to perform routine functions with the Proxy Player in *Shotlist Mode* on the **Admin, System, Shortcuts, Shotlist** screen in the navigation tree on the left side of the screen. Click the **Pencil** icon to edit existing shortcut combinations.

Proxy Player Shortcuts

The Proxy Player is the default player mode. You configure hot keys used to perform functions with the Proxy Player in the default *Play* mode on the **Admin, System, Shortcuts, Player** screen in the navigation tree on the left side of the screen. Click the **Pencil** icon to edit existing shortcut combinations.

Next you will add your organization's logo.

Style

If required, you can quickly customize the interface style with an organizational logo that appears on all GUI screens in the top right corner of the screen. Use the following procedure to add a logo:

1. Navigate to the **Admin, System, Style** screen on the navigation tree on the left side of the GUI.
2. Click **Browse**, and then navigate to the desired image file in the *Browse* dialog box.
3. Select the desired file, and then click **OK**.
4. Click **Save** on the top right side of the screen to apply the changes.
5. Refresh the browser screen to view the changes.

Next you will configure the DIVAdirector Web Server.

Configuring DIVAdirector Web Server

DIVAdirector uses Microsoft Internet Information Server (IIS) 7 as the web server engine. IIS is installed during Windows Server 2008 R2, and 2012 R2 installation.

The DIVAdirector Web Server is fully configured by the installation application. There is no need to adjust the configuration unless specific web server parameters require modification. The default IP port is port 80 and will bind to the first network adapter in the system device list. Contact Oracle Support if you need assistance binding the server to a different network adapter.

First you will configure the Listening Port.

Listening Port Configuration

The default listening port value is 80. This is the standard internet HTTP port for web servers. This value may be any port number not being used in the system, and should be changed if port 80 is unavailable. IIS must be restarted from the command line using the `issreset` command to apply a change to the port number.

Note: After changing the server to a nonstandard port number, DIVAdirector users may be required to explicitly specify the port number in the web address, for example, `http://dd5server:8080`.

If changes are made to the listening port, test the web server configuration by opening your web browser and entering the DIVAdirector IP address and port number (if required) in the URL Address field.

Next you will configure the IIS Service Account.

IIS Service Account Configuration

The DIVAdirector installation process creates an account named `dd5-user`. Oracle recommends that you run IIS using a domain account. *See the Oracle DIVAdirector Installation Guide for more details.*

Next you will configure accounts.

Account Configuration

DIVAdirector is a permission based system that allows a limited number of simultaneously logged in users. This number of concurrent users depends on system resources and the maximum configurable value is 100 concurrent users. Any user accessing the system must be validated through the log in procedure. To be authorized to access the system, the user must enter a valid login username or email address and password specific to the user account.

There are three tiers of access control in DIVAdirector which are structured as follows:

Organizations

This category is the top level account for different internal departments. Organizations are comprised of groups.

Groups

This category is the second level account for different groups within an organization. Groups are comprised of user accounts.

Users

This category is the third level account for individual system users. Users are members of groups.

First you will configure a new organization.

Adding an Organization

Organizations are comprised of a set of groups. Organizations allow restricting access to information from users outside of the organization or group who do not require access to the data. For example, a company may not want to make its data viewable to other companies, or a department within a company may not want its data to be viewable by other departments within the same company. In these two scenarios, the

entire company, or the specific department, desiring restricted access can be represented by an organization in DIVAdirector.

Use the following procedure to create an organization:

1. Navigate to **Admin, Users, Organizations** in the menu on the left side of the screen.
2. Click the + next to the **Users** menu item to expand the menu tree.
3. Select **New Organization** in the *Organization* list.
4. Enter the Organization Name in the *Organization Name* field.
5. Enter the LDAP settings in the *LDAP Settings* field if an LDAP login is required.

If your organization uses **LDAP (Lightweight Directory Access Protocol)**, you can configure DIVAdirector users so they log in to the system using LDAP. Your administrative account should never be configured to use LDAP login because if the LDAP server address is incorrect, or the LDAP servers become unavailable, nobody (including you) will be able to log in. You are only able to log in using DIVAdirector's user name and password log in mechanism, which enables resetting the LDAP settings if the servers become unavailable or the settings had been incorrectly specified.

You can specify a port number by suffixing the IP address with the `:port` option. The port is the port number for DIVAdirector to listen for LDAP connections. If no port is specified, the default LDAP Port (port 389) is used. You can also specify an optional secondary LDAP server address (and port number if required) for authentication in case the primary server fails or is unreachable.

6. Enter SMTP Server information in the SMTP related fields (if applicable). Enabling SMTP allows users the ability to recover lost passwords through email.
7. In the Permissions' Content Filters area enter any *Objects, Categories* and *Sites* - multiple entries are separated by a semicolon. Use an asterisk to denote wildcards (for example `ABC*` or `AB*D`, and so on). An exclamation point preceding any filter implies that only objects determined by that filter should be included.

The site permissions are extremely important because they allow the organization to access objects on specific sites that match the filter.

8. Identify the *Metadata Access* fields that will be accessible by the organization by selecting the check box to the right of the metadata name. If the check box is deselected the organization will not have access to that metadata field. Groups within an organization may further refine their authorized selections.
9. Click on the **DIVArchive Settings** Tab. Add any Source/Destinations, Storage Plans, or Media this organization should have access to. Groups contained within this organization will only be permitted the ability to grant access to each resource defined here.
10. Click **Save** on the top right side of the screen to save the information.

Next you will add a new group.

Adding a Group

Groups are collections of users and part of an organization. Each group is assigned a set of permissions to grant users of the group access to specific system features and functions. Groups are customizable and are configurable to fit organizational security requirements. By default, the system is installed with two user groups - *SystemAdmins* and *admins*.

The SystemAdmins group is the most powerful group in the system, and has special privileges to access all configuration elements of the system. Users who are members of the SystemAdmins group are the only users who have complete access to all permissions, configuration parameters, queries, Work Bins, and Shot Lists for every other user in the system.

When creating a new group you assign the new group a unique name. Group names should be descriptive and unambiguous to make further system administration and maintenance simple and clear. Group names must not exceed 32 characters.

Use the following procedure to create a group and set the group's permissions:

1. Navigate to the **Admin, Users, Groups** screen. The screen will initially display with the **Profile** tab selected.
2. Select **New Group** from the *Group* list.
3. Enter a new group name in the *Group Name* field.
4. Select the group's organization from the *Organization* list.
5. Click **Save** on the top right of the screen to create the new group.

Group Roles

Now that you have created the group and associated it with the correct organization, you must identify the roles for the group.

All users, regardless of their group's roles, always have access to the **Operation Status**, **Change Password**, and **Logout** functions. Only SystemAdmins have access to the *Organization* screen, *Shortcuts* screens, *Public Resources* screen, and the *Proxy Configuration* screens.

Use the following procedure to set the group member's roles:

1. Navigate to the **Admin, Users, Groups** screen.
2. Click the **Permissions** tab to view the *Permissions* screen.
3. Configure the appropriate roles for the group using the check boxes in the *Privileges* area.

A selected check box indicates that the group has been granted permission to that function. A deselected check box indicates that the group has been denied permission to the function.

4. Click **Save** on the top right of the screen to save the new group and its associated permissions.

The following sections describe the different permissions available for groups.

General Privileges

You can enable or disable the following general group privileges:

View Queries and Save Advanced Searches

Allows users to view and save queries they performed, or were shared by a group they have access to.

Create and View Work Bins

Allows users to create personal and public work bins and perform actions within them.

Use Group Drop Folders

Allows users to create and use group defined Drop Folders.

Modify Asset Metadata

Allows users to modify the object metadata within the *Edit Metadata* page. If this permission is disabled, the metadata is displayed to the user in a read-only format.

Create Shot Lists

Allows users to access the *Shot List* screen, add objects and segments of proxies, and perform file management and editing operations. If the user does not have this permission, **Edit** (and the icons) will not be displayed on the *Query Results* and *Work Bin* panels, and the **Shot List** menu item will not be displayed.

Publish Shot Lists

Allows users to create their own public *Shot Lists*. If this permission is disabled, *Make Public* will not be displayed on the *Shot List* panel.

View Asset Proxies

Allows users to view the proxy and also enables **Play**.

Download Proxies

Allows users to download proxy videos to their local system.

Modify Annotations

Allows users to have the ability to add, edit, and delete annotation metadata.

Manual Proxy Generation

Allows users to request generation of a proxy for an object. The generation uses the rules defined in the **System, Proxies, Proxy Generation** page.

DIVArchive Operation Privileges

You can enable or disable the following DIVArchive group operation privileges:

Archive from Source

Allows users to archive new data to the DIVArchive long term storage.

Delete

Allows users to delete object instances from the DIVArchive long term storage.

Restore

Allows users to restore objects from the DIVArchive long-term storage so they are available for immediate access on the specified destination (for example an FTP destination, or a video server).

Partial Restore

Allows users to perform Partial File Restore operations on the selected file in the *Shot List*.

Local Archive

Allows users to upload content from their local system to a staging location associated with their user name on the Local Archive Source/Destination.

Local Restore

Allows users to restore files and to download directly from the *Operation Status* page.

Local Partial Restore

Allows users to partially restore files and to download directly from the *Operation Status* page.

Create Virtual Assets

Allows users to create virtual objects.

Local Proxies

Allows users to upload files to a Proxy Drop Folder that has been configured to automatically extract metadata and proxy frames.

Note: Continued use of proxies produced outside of DIVAdirector and DIVArchive for local proxies will continue to function, but is highly discouraged.

Administration Privileges

You can enable or disable the following group administration privileges:

User Management

Enables the configured group to manage users through the Admin, Users, User page.

Start Proxies In Paused Mode

Enabling this will prevent the auto playback of proxies when navigating through the Shotlist page.

Modify Metadata Schema

Enables users to access the **Admin, Metadata** screen to manage *Asset Metadata* fields by viewing, editing, adding, and deleting metadata columns.

Modify Interface Style

Enables users to access the **Admin, System, Style** screen, and to upload a new banner logo image. The banner logo image is used for customizing the look and feel of DIVAdirector by adding an organization's logo on the top right corner of all pages.

Display Site Information

Enables or disables viewing of the site information for objects.

Allow Group-Wide Access (Implies User-Wide Access)

Enables users to configure and create groups within an organization. The groups created will not have access to any system administration privileges unless they have been explicitly granted by a SystemAdmin. Each member of the group will also be able to see queries, *Work Bins*, and *Shot Lists* of every other user within the user's organization.

Allow User-Wide Access

Enables users to modify and create user accounts within a group. Each member of the group will also be able to see queries, *Work Bins*, and *Shot Lists* of every other user within the group.

Administer Dropfolder

Allows users to create new Drop Folders, and modify existing ones.

System Administration Privileges

You can enable or disable the following group system administration privileges:

Discover Objects and Manage Requests

Grants users access to administrative functionality for synchronization and managing system requests. Request management is performed on the *Operation Status* screen and enables users with this permission to manage the request priority or cancel requests in the system.

Modify Policies and Settings

Enables users to edit the default system settings (located on the **System, Defaults** screen), settings under the *Service Settings* page, and the *Public Resource* page.

Administer Database Backups

Enables users to access the *Perform Database Backup Operations* area located on the **Admin, Backup** menu. Backup operations include viewing the last operation, scheduling an automatic backup, and performing a manual backup or restore.

Allow Audit Trail

Enables or disables the audit trail. The audit trail is located on the **System, Audit Trail** screen.

Session Management

Enables or disables session management. The session management is located on the **System, Session Management** screen.

Modify Storage Locations

Enables users to access the *Storage Locations* page located under **Admin, System**.

Modify Proxy Generation Settings

Enables users to access the *Proxy Generation* page located under **Admin, System, Proxies**.

Modify Proxy Migration Settings

Enables users to access the *Proxy Migration* page located under **Admin, System, Proxies**.

Modify Transcoder Settings

Enables users to access the Transcode Service pages located under **Admin, system, Service Settings**.

Content Filters

Group based filters are configured on the *Permissions* screen. Any changes made and saved in the filters are applied immediately for all currently logged in users associated with the group. The Content Filter enables users to see only data complying with a set of filters for Object Name, Object Category, and Sites.

The Content Filter is a table with three fields at the bottom of the *Permissions* screen. All of the fields in the table are initially empty. An empty field indicates that no filtering will take place for that type of discriminator. The content filters are applied to both queries and *Work Bins*, but do not affect *Shot Lists* and the *Status* screen.

Each field can have multiple filters separated by semicolons. An asterisk is used as a wildcard symbol. An exclamation point at the beginning of a filter indicates that only items that match the filter should be included, while the lack of an exclamation point indicates an exclusion. The filter can also be blank or have white space indicating that no filtering is required; white spaces between filters are ignored.

Note: Organization level filters are also applied with, but are obfuscated, from the group level configuration.

Metadata Permissions

Use the Permissions (Metadata) tab to configure Metadata Permissions for a given group. There are two types of permissions:

- Access — grants the group the ability to see and manipulate the associated metadata field.
- Publish — grants the group permission to send the selected metadata to a DIVApublish server.

Note: Only metadata that the containing Organization has been granted access to will be visible in this list.

Next you will configure DIVArchive operational parameters.

DIVArchive Operations

The parameter values for the following DIVArchive operations are configured on the **DIVArchive Settings** tab on the **Admin, Users, Groups** screen. Not all parameters are applicable to all operations. Valid operational parameters are as follows:

Archive

Valid parameters are *Source, Media, Storage Plan, QoS, Priority, and Category*.

Local Archive

Valid parameters are *Source, Storage Plan, QoS, Priority, and Category*.

Restore

Valid parameters are *Destination, QoS, and Priority*.

Local Restore

Valid parameters are *QoS and Priority*.

Partial File Restore (PFR)

Valid parameters are *Destination, QoS, Priority, File Format, and PFR Name Format*.

Delete

Valid parameter is *Priority*.

The valid parameters for each operation are applied according to the following descriptions:

Source

The *Source* parameter defines a list of DIVArchive source storage locations for DIVArchive operations. Users only see the selected sources in the list. Whichever DIVArchive source is chosen to be the default will appear as the default item in the user's list.

Destination

The *Destination* parameter defines a list of DIVArchive destination storage locations for DIVArchive operations. Users only see the selected destinations in the list.

Whichever DIVArchive destination is chosen to be default will appear as the default item in the user's list.

Media

The *Media* parameter defines a list of DIVArchive media for DIVArchive operations. Users only see the selected media in the list. Whichever DIVArchive media is chosen to be the default will appear as the default item in the user's list.

Storage Plan

The *Storage Plan* parameter defines a list of DIVArchive Storage Plans for DIVArchive operations. Users only see the selected Storage Plans in the list. Whichever DIVArchive Storage Plan is chosen to be the default will appear as the default item in the user's list.

Quality of Service (QoS)

The *QoS* parameter defines the Quality of Service for DIVArchive operations. The available choices are **Default**, **Cache**, **Direct**, **Cache and Direct**, and **Direct and Cache**. If the *Force Default Value* check box is selected, the chosen option cannot be changed by the user before executing an operation.

Priority

The *Priority* parameter defines the execution priority of DIVArchive operations. This parameter has a minimum value of 0 and maximum value of 100 (100 is the highest priority). If the *Force Default Value* check box is selected, the chosen option cannot be changed by the user before executing an operation.

Category

The *Category* parameter defines a list of object categories for DIVArchive operations. Only the selected categories will be included in the user's list. The list will initially be empty; clicking + allows new categories to be added.

File Format

The *File Format* parameter defines the format of the high-resolution files stored in DIVArchive for Partial File Restore operations.

PFR Name Format

The *PFR Name Format* parameter defines the file name format for files displayed in the Partial File Restore operation results. The first list contains the types of separators used in the name format (underline, dash, or period). The second list contains additional name construction types as follows:

- **none**: the object name is used as the file name; additional construction is not used.
- **1**: one digit of the segment number in the *Shot List* is added to the file name with the separator (for example, `objectname_1.gxf`).
- **2**: two digits of the segment number in the *Shot List* are added to the file name with the separator (for example, `objectname_01.gxf`).
- **3**: three digits of the segment number in the *Shot List* are added to the file name with the separator (for example, `objectname_001.gxf`).
- **4**: four digits of the segment number in the *Shot List* are added to the file name with the separator (for example, `objectname_0001.gxf`).
- **SOM-EOM**: time codes are used in the file name (for example, `{objectname_start-timecode-of-segment}-{end-timecode-of-segment}.gxf`).

The *Use Relative TC* check box determines whether relative or absolute timecodes are used in the PFR File Name construction and the Partial File Restore operation.

Next you will configure data export roles.

Data Export

You choose the data export settings for the group from three lists on the **Export Settings** tab. The lists are as follows:

Default Shot List Export Video Format

This list determines the video format in an EDL export file. Select either **NTSC** or **PAL** from the list.

Default Shot List Export Format

This list determines the *Shot List* export format. Select from either **Final Cut Pro** or **Avid ALE**.

Default Metadata Export Format

This list determines the metadata export format. Select from either **CSV** or **XML**.

Next you will add a new user.

Source/Destination Configuration

In DIVArchive and DIVAdirector, a Source/Destination is a disk or server that DIVArchive can archive from or restore to. The difference is in the actions being performed. For example, *Tape Storage-A* can be defined as a source for Restore or Partial File Restore operations. However, *Tape Storage-A* can also be designated as a destination for Archive and Copy operations. You configure the storage locations and identify them as a source, a destination, or both in DIVArchive. DIVAdirector will use the storage locations as they are identified in DIVArchive.

Adding a User

All users are members of a group and inherit the roles and accesses assigned to the group. You add new users to the system using the following procedure to create a user account:

1. Navigate to **Admin, Users, User** in the navigation tree on the left side of the screen.
2. From the *User* list select **new user**.
3. The following information is mandatory and entered in the *Account Information* area. All other fields are optional and may be left blank if desired.

User Name

Enter the desired user name. Users can log in using either the user name or the email address. User names must be unique within the system.

Group

Select the organizational group to which the user will belong from the list.

Email

Enter the email address to be used for logging in to the system. This is not case sensitive.

Lockout Status

You should leave this selection set to **Not Locked** when you create the user. An administrator can lock users out of the system at any time by changing the value of this parameter.

There are two types of lockouts that can occur:

A normal *Locked* status occurs from login failures, and can be resolved by a password reset link sent by email or by contacting an administrator.

A *Locked By Administrator* status means that all attempts to gain access to the system will fail. This status only occurs when an administrator selects this status for a user.

Note: The system ignores the *Lockout Status*, other than *Locked By Administrator*, when you configure LDAP for an organization.

Temporary Password

Enter an initial password to be used for logging in to the system for the first time. Passwords must conform to the following rules and expire every ninety days:

- Passwords must be between 8 and 128 characters in length.
- Passwords must contain a letter, number and a symbol.
- Passwords must not contain white space characters.
- New Passwords must not be any previously used passwords.

Confirm Password

Re-enter the user's password to confirm it is correct. This must match the *Temporary Password* field exactly.

Note: The *Temporary Password* and *Confirm Password* fields display only asterisks for security purposes rather than clear text.

4. Click **Save** on the top right side of the screen to create the new user.

Next you will configure sources and destinations.

Drop Folder Configuration

Drop Folders are directories on a storage location where you can place (drop) files to perform preconfigured tasks. While these tasks can be performed through various areas in the Web Interface, Drop Folders bypass the need for navigating a UI and can aggregate similar work into one simple action.

DIVAdirector actively monitors each Drop Folder for new files on disk and also has a Web Interface you can use to drop files and folders. The Web Interface section is located under the **Dropfolders** panel in the navigation tree. A given Drop Folder's visibility in the Web Interface is configured on a per group basis. Through the interface you may view each Drop Folder task status and any associated logs. Of the four types of Drop Folders available, there are three that are configurable; *DIVArchive*, *Metadata*, and *Proxy. Annotation* Drop Folders have a preset configuration as described in another section.

The *Dropfolder Configuration* page is located under the **Admin** navigation tree.

To configure Drop Folders you must have the appropriate configuration permission. You can enable (or disable) this permission as follows:

1. Navigate to the **Admin, Users, Groups** page using the navigation tree on the left side of the screen.

2. Select **admin** from the *Groups* list.
3. Click the **Permissions** tab.
4. Select the *Administer Dropfolders* check box under the *Administration* area to enable permission to configure Drop Folders.
To disable permission deselect the Administer Dropfolders check box.
5. Click **Save** to save your changes.

After you have the correct permission, you configure the following Drop Folder options on the *Dropfolders Configuration* screen under **Menu Options** on the top right side of the screen:

Save

Clicking this menu item saves the currently selected configuration.

Import

A file selector prompt will initiate the Drop Folder configuration import process. Both legacy XML formatted Drop Folder configurations, and new configurations are supported. After you import a configuration you must identify the *Watch Path* option and any other necessary configuration values before saving the configuration. Options will not be imported if the current group does not have access to them. For example, you cannot import metadata fields that your group does not have permission to edit.

Delete

Clicking this menu item deletes the currently selected configuration.

Export

Clicking this menu item exports, and then downloads, the current Drop Folder configuration in XML format.

You can configure the following Drop Folder options on the *Dropfolders Configuration* screen under **Drop Folder Configuration Options**:

Folder Settings - all of the following options are required:

Drop Folder Type

The type of Drop Folder dictates which configuration options are available.

Action (DIVArchive Drop Folders Only)

This determines the type of DIVArchive action to perform and the configurable options available. The types of actions are as follows:

Archive

This action encompasses all types of Archive actions.

Restore

This action encompasses all types of Restore actions including file based Partial file Restore and timecode based Partial File Restore.

Copy

This action enables the copying of assets to different media.

Purge

This action enables delete type actions for both single instances and full asset deletion.

Description

This is the title that is reflected in the navigator and the name of the export file when the Drop Folder is exported.

Watch Path

This parameter is the full path that the Drop Folder Monitor uses to look for new files to process. You cannot modify the *Watch Path* after a Drop Folder is configured and saved.

Log File Path

This parameter identifies the full path on the DIVAdirector Server that contains the individual log files for each file processing attempt.

Group Assignments

This parameter identifies the currently assigned groups allowed to see this Drop Folder through the user interface. Drop Folders that do not have any group assignments will still be active, but will only be available to ingest files from the file system.

Add Group

This parameter is a list of available groups to assign. The list will only contain groups within the same organization as the logged in user. Only the `SystemAdmin` account can see all groups at once.

Enabled

Selecting this check box enables the configured Drop Folder. Deselecting the check box disables the configuration

File Process Settings:

File Format Type

The value in this field defines the file format the Drop Folder is expecting.

CSV

Selecting this value displays the configuration options required to define the schema (see the following details).

XML (Metadata Drop Folders Only)

XML formatted metadata can be ingested provided the XML format guidelines are followed (see the following details).

JSON

This format is not currently implemented.

File Encoding

This parameter identifies the configuration of the expected ingest files encoding. Confirm that these encoding settings are correct to properly ingest character sets outside of the ASCII standard.

Save Backup File

Selecting the check box for this option will save a copy of the ingested file in case there were any errors detected in processing.

Backup Path

This parameter identifies the full path on the server where backup copies are made in case an error in processing occurs. *This field is required if the **Save Backup File** check box is selected (the option is enabled).*

CSV File Format Settings:

Delimiter

Importing CSV files supports using one of three delimiting characters; comma, semicolon, and tab.

Encapsulation

An encapsulation character enables the use of a delimiting character within the metadata value. Currently the only encapsulation character supported is a quotation mark. If an encapsulation character is present within the imported metadata, it must be escaped with a backslash.

Has Header Row

When this check box is selected it indicates that the CSV has a one line header at the top of the file that must be ignored by the parser.

Category Matching

This parameter enables matching a CSV row to objects without supplying a category within the dropped file. You can achieve matching through a list of categories, or all categories, if the *Use Only Object Name* check box is selected.

Note: When a proxy drop folder is configured with this setting, the drop folder will assign the proxy based on a matched file name convention for objects that only contain one file.

DIVArchive Operation Drop Folders

DIVArchive Drop Folders allow you to execute large numbers of DIVArchive requests based on the folder configuration. The volume of requests submitted simultaneously is throttled to avoid overwhelming the archive system. You can perform four types of actions including Archive, Copy, Restore and Purge. All dropped CSV files must contain a field for *Object Name*. Depending on the *Category Matching* settings previously described, a column defined for *Object Category* may also be necessary.

DIVArchive Request Processing Settings:

Max DIVArchive Queue Size

This option sets the maximum number of active processing requests before the Drop Folder will pause any new submissions.

Request Set Size

This option defines the number of requests to send per sleep interval.

Sleep Interval

This option determines the length of time before sending new requests or checking the status of the DIVArchive processing queue.

Priority

This option sets the priority level of requests submitted to DIVArchive. Requests with higher priority take precedence over requests with lower priority. *This option can be overridden as part of the dropped CSV.*

Archive Action

DIVArchive Request Settings (All request settings can be overridden as part of the dropped CSV):

Source/Destination

This option identifies the originating Source of a request. You can provide specific log in credentials associated with the source. You can also set a flag for deleting archived files after the request is processed.

Media

This option identifies the Media Name or Storage Plan for the archived asset.

Quality Of Service

This option identifies the Quality of Service for the archive request. *See the Oracle DIVArchive documentation for further information.*

Root Path

This option identifies the root path of the Archive request such that the file list will contain relative paths to this root.

Archive Comments

This option is the comments field of the archive request. You cannot edit comments after they are submitted and they are attached to the resulting objects metadata.

*Additional CSV Field Mappings***List of Files**

This option is a semicolon delimited list of files to archive. Files must use a relative path from the root path if it is set or the base of the source if it is not. You can use an asterisk wildcard to indicate a recursive archive from a folder path.

Copy Action

DIVArchive Request Settings (All request settings can be overridden as part of the dropped CSV):

Media

This option identifies the Media Name or Storage Plan to copy an object.

*Additional CSV Field Mappings***Instance**

This option identifies an instance number to perform the object copy from.

Restore Action

DIVArchive Request Settings (All request settings can be overridden as part of the dropped CSV):

Source/Destination

This option identifies the restore destination of a request. You can provide specific log in credentials associated with the destination.

Quality Of Service

This option identifies the Quality of Service for the archive request. *See the Oracle DIVArchive documentation for further information.*

Additional Restore Options (Cannot be overridden by the CSV file)

You can indicate what actions to take on the Restore request. For example, you may want to prevent overwriting existing files on the restore location, or conversely, make sure the existing files are deleted first.

Root Path

This option identifies the root path of the Restore request such that the file list will be restored to a specific folder within the destination.

Additional CSV Field Mappings

List of Files

This option identifies a semicolon delimited list of files to restore. You can use an asterisk wildcard to indicate a Recursive Restore from a folder in the object file list.

Instance

This option identifies an instance number to perform the restore operation from.

Mark In

This option identifies a *Mark In* timecode in SMPTE format for a timecode based Partial File Restore. If you also enter a *List of Files* value, DIVArchive will attempt to perform a timecode Partial File Restore on each file.

Mark Out

This option identifies a *Mark Out* timecode in SMPTE format for a timecode based Partial File Restore. If you enter a *List Of Files* value, DIVArchive will attempt to do a timecode Partial File Restore on each file.

Purge Action

DIVArchive Request Settings (All request settings can be overridden as part of the dropped CSV):

Media

This option identifies sets the media name to delete instances of an object from. This field is optional.

Additional CSV Field Mappings

Instance

This option identifies a specific instance number to delete. If neither an *Instance* or *Media* is defined, the process deletes the entire object from the archive system.

Metadata Drop Folder Configuration

Action Settings:

Overwrite Old Data

This option overwrites existing metadata if an object already has metadata defined in the specified field.

Delete On Null

This option removes specified metadata from an object if an empty value is parsed from the processed file.

Virtualize

This option creates virtual objects if metadata is added to an object that does not currently exist in the archive.

Field Mappings (CSV Specific)

Field mappings identify the order of the columns defined in your CSV file. You can reorder defined mappings by dragging and dropping the fields into the desired positions. Every CSV import requires the predefined fields *Name* and *Category*. You can add fields by clicking the + button. This displays the *Field Mappings* dialog box.

The *Metadata Type* list will only include fields that have not already been added to the Drop Folder, and metadata types that the group has access to. You can define the *DateTime Mask* field for date or time metadata. However, if no mask is specified, a generic format will be used. You can edit edited or delete fields at any time by clicking either the **Pencil** or **X** icons respectively.

The *Space Removal* option enables trimming of white space from your provided file.

Note: *DateTime Masks* use standard formatting strings. You can find a full list of possible options at [https://msdn.microsoft.com/en-us/library/8kb3ddd4\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/8kb3ddd4(v=vs.110).aspx).

XML Formatting:

The following example shows the required XML formatting:

```
<DIVADirectorMetadataXML>
  <Category object_category="a_category">
    <Object object_name="an_object_name1">
      <Item metadata_name="metadata_field1">
        <Value>Data</Value>
      </Item>
      <Item metadata_name="metadata_field2" dt_mask="MM/dd/yyyy">
        <Value>01/01/2017</Value>
      </Item>
    </Object>
  </Category>
</DIVADirectorMetadataXML>
```

Annotation Drop Folders

Annotation Drop Folders allow the importation of commented segments for files within objects. The CSV's that are dropped with this type of folder have a predefined structure as follows.

Object Name

This column is limited to 240 characters and should match the object name in DIVArchive.

Category Name

This column is limited to 240 characters and should match the object category name in DIVArchive.

Object File Name

The filename within the object to add the segment to.

Start Time Code

Start time of the locator in the format hh:mm:ss:ff.

End Time code

End time of the locator in the format hh:mm:ss:ff. This field is not mandatory and if left empty, the locator is considered a marker (description of a single frame).

Description

The text description of the segment, limited to 2000 characters.

Adding Proxy Drop Folders

Note: Oracle recommends using the new transcode service rather than Proxy Drop Folders. Continued use of proxies produced outside of DIVAdirector and DIVArchive for local proxies will continue to function.

All proxies registered in the DIVAdirector system are kept on Proxy Storage Locations. These are configured in the **Admin, System, Proxies** section of the web interface. By default, one proxy location is added during DIVAdirector installation. However, you can configure and manage multiple proxy storage locations.

The *Proxy Storage Location* is defined by the path to the folder on the file system (either a local location or network share). The default location will be the `C:\Program Files\DIVAdirector\proxies` folder. During a custom installation the location will be a folder selected by you.

Each location has limited usable space on the storage device, either relative or fixed. A relative limit is set as a percentage relative to the capacity of the storage device, while a fixed limit is set in megabytes.

The **Proxy Storage Location** control enables viewing of the following information about each proxy location:

State

This field displays the current state of the proxy location.

Physical Path

This field displays the path to the proxy location folder.

Virtual Path

This field displays the path used by the web application to access the storage location. On most installations, this will be `DIVAdirector Proxies`.

Available Space

This field displays the space available in the proxy location.

Limit Type

This field displays the type of limit (bytes or percent) used to configure the storage location.

Limit Value

This field displays the amount of space that can be used on the storage device.

Map the Storage Location in Windows and Set Folder Permissions

Use the following procedures to add a Proxy Storage Location:

1. Map the storage location so it is visible in Windows.
2. If the folder is a network drive, confirm it is set to reconnect on Windows start.
3. In Windows File Explorer, right-click the folder, and then select **Properties** from the menu.
4. Click **Edit** in the middle of the *Security Tab* screen.

5. Click **Add** in the middle of the screen to add a user to the folder's permissions.
6. When the *Select Users or Groups* dialog box appears, enter the IIS web server account (the default is `dd5-user`) used during DIVAdirector installation in the *Object Name* field (on the bottom of the screen), and then click **Check Names** to verify that the entered name is valid.
7. When the user is verified, click **OK** to add the user.
8. Repeat Step 5, Step 6, and Step 7 for *Authenticated Users*. Both users are now added to the folder permissions and set correctly for the DIVAdirector Web Server.

Add the Proxy Folder to the DIVAdirector Web Server in IIS

Use the following procedure to add the proxy folder to the DIVAdirector Web Server in IIS:

1. Open the IIS Manager application (`inetmgr`).
2. On the left side of the IIS Manager click the host's **Computer Name** under the **Sites** menu, and then click **DIVAdirector 5**.
3. Right-click **DIVAdirector 5**, and then select **Add Virtual Directory** from the resulting menu.
4. Enter the *Alias* (virtual path) and *Physical Path* of the new proxy storage location.
5. Click **OK** to complete the process.

Configuring the Proxy Storage Location

The **Storage Location** configuration is located in **Admin, System, Proxies** screen. Add a new Storage Location with the same physical and virtual path created in IIS in the previous steps using the following procedure:

Note: The *Proxy Location Path* cannot be changed after it has been added.

1. Click the **Add** under the *Storage Locations* header.
2. Enter the same physical path used to setup the virtual directory in IIS in the *Physical Path* field.
3. Enter the same alias used to setup the virtual directory in IIS (usually `DIVAdirector proxies`) in the *Virtual Path* field.
4. Select either **Bytes** or **Percent** from the *Limit Type* list.
5. Enter a value in the *Limit Value* field.
6. Click **Update** to save your configuration.

After saving the configuration, the state of the storage location will be updated to one of the following values:

Open

This status indicates that the limit value has not been reached for this storage location. Open locations can accept new files.

Closed

This status indicates that this storage location does not accept new files. A **Closed** location can be explicitly transitioned to the **Open** state only.

Overflown

This status indicates that the limit value has been reached for this storage location. **Overflown** locations do not accept new files and cannot be transitioned to another state.

Unreachable

This status indicates that the storage location is not currently detected in the environment (the path is not found). An **Unreachable** location cannot be transitioned to another state or removed.

Add Proxy Drop Folder

You must configure a new Proxy Drop Folder in the **Admin, Dropfolder Configuration** section after you have created the virtual directory in IIS, and configured the *Storage Location*. Use the following procedure to create the Proxy Drop Folder:

1. Select **Create new Folder** from the menu list at the top of the screen.
2. Select **Proxy** from the *Dropfolder Type* list.
3. You can configure the remaining fields in the panel on the left side like other folders described in [Drop Folder Configuration](#).
4. To have a transcoder workflow create the Proxy Key Frames and metadata, check 'Automatically Generate' and then select a workflow from the drop-down.

If you chose to not automatically generate these, you can manually add the Proxy Key Frames to a folder labeled 'Keyframes' in a relative path to the proxy location. Then, to add the metadata, you can create a 'metadata.json' file in the same location to the proxy.
5. You may opt to create a Proxy Drop Folder based on file naming convention, where just the proxy is dropped into the drop folder. This configuration will only work for objects that have a single file within them. You must also configure the Automatic Generation of Proxy Key Frames and metadata in order to use this option.
6. Click **Save** in the upper right corner to save your changes.

Proxy Drop Folder File Format

DIVAdirector associates proxies with files in an object, instead of the object itself. It is also possible for multiple proxies to be associated with a single file. This is a new feature starting with DIVAdirector 5.4. To support this functionality, proxies dropped into a Proxy Drop Folder require a *Manifest File* associated with them. The *Manifest File* triggers the proxy creation process. The *Manifest File* is a `.csv` file that associates an object name, category, and file with a proxy file. The following fields are required:

ObjectName

This parameter identifies the object name containing the file that will have a proxy associated with it.

ObjectCategory

This parameter identifies the object category containing the file that will have a proxy associated with it.

ObjectFile

This parameter identifies the object file that will have a proxy associated with it. This is the relative path of the object file in the object file hierarchy. For example, `sub1/sub2/file1.mxf`.

ProxyFilePath

This parameter identifies the full file path of the low resolution proxy file that will be used by DIVAdirector.

ReplaceProxies

This parameter identifies a boolean value specifying if existing proxies should be replaced with the current one. If this value is `false`, additional proxies will be created for that object file when *Manifest File* for that object name, category, and file are processed. If this value is `true`, then any proxies for that object file will be removed and replaced with the one specified in the *Manifest File*.

Language

This parameter identifies a string value defining the language track to use in audio proxy files.

The addition and configuration of the new location is now complete. Test the new location by dropping a proxy file into the folder as a non-administrative user, and then open the file with the Proxy Player.

Proxy Generation

Proxy generation is configured in the **Admin, System, Proxies, Proxy Generation** area. This section is only available to users in groups that have the *Modify Proxy Generation Settings* permissions. Before configuring this section, follow the steps in [Configuring the Proxy Storage Location](#) to create a location to store proxies.

Adding Category Filters

You can add Category filters to control which object categories will have proxies created for them, which files they can be associated with, and where the generated proxies will be stored. Use the following procedure to assign a category filter:

1. Click **Add** in the *Category Filters* section.
2. Check the "Enable Full Restore" checkbox to send a full restore request for each object in the selected category filter. If this checkbox is left unchecked, then a partial file restore request will be sent for the selected proxyable file(s).
3. Check the "Proxy All Files" checkbox to generate a proxy for each file matching the "Proxyable file extensions" filter.

Note: There is a limit of 100 proxies per object. If this checkbox is left unchecked, then only one matching the "Proxyable file extensions" will be selected for proxy creation.

4. Select the category name that should have proxies created for it from the list. You can select the asterisk if the filter should apply to all categories.

5. Select the storage location where the proxies should be stored. You can select the asterisk here if multiple storage locations have been defined and you want to use the default filling strategy.
6. Enter the file extensions that should have proxies created for them. This is a comma separated list of file extensions (for example, `mx.f`, `mov`, `mp4`, and so on).
7. Select the transcoder workflow to use for proxy generation.
8. Click **Update** to save the filter.

DIVArchive Restore Options

Next, you must configure the DIVArchive options used to restore the source file. These restore options will also be used for manual proxy generation tasks. At the top of the section on the right, locate the *DIVArchive Restore Options* panel, and configure the following values:

Restore Destination

This field identifies the Source/Destination where files will be restored.

Files Path Root

This field identifies the folder under *Restore Destination* where files will be restored.

Qos

This field identifies the Quality of Service parameter issued to the DIVArchive Restore request.

Priority

This field identifies the priority parameter issued to the DIVArchive Restore request.

Options

This field identifies any additional parameters that need to be issued to the DIVArchive Restore request.

Scheduling

You can configure proxy generation to run continuously or only within a specified period. You configure these settings in the second section on the right side of the screen. In the *Schedule* panel, a list of check boxes and time selectors are displayed next to each day of the week.

To have the proxy generation task run continuously, deselect the check box next to each day of the week. To constrain the generation task to run within a certain period, select the check box next to the desired day of the week and the appropriate start time and end time.

Click **Save** at the top of the page when configuration is complete. Click **Start** in the *Task History* section to start the generation task.

Proxy Migration

You can use the proxy migration process to convert legacy proxy formats (for example, WMV) to a newer format (MP4). This process is configured under **Admin, System, Proxies, Proxy Migration**, and is only available to users in groups that have the *Modify Proxy Migration Settings* permissions. Before configuring this section, follow the steps in [Configuring the Proxy Storage Location](#) to create a location to store proxies.

In the top section under *Legacy Proxies*, a summary is displayed showing the counts of legacy proxy formats. Beneath that is a section for configuring the object categories that will have legacy proxy formats migration. The process for configuring these categories is similar to configuring proxy generation.

You can add category filters to control which object categories will have proxies migrated for them, which files they can be associated with, and where the migrated proxies will be stored.

Use the following procedure to configure category filters:

1. Click **Add** in the *Category Filters* section.
2. Select the category name that should have proxies migrated for it from the *Category Name* list. You can select the asterisk if the filter should apply to all categories.
3. Select the storage location where the proxies should be stored from the *Storage Location* list.
4. Click **Update** to save the filter.

Set the queue size to update the number of concurrent migrations that will occur in the top section on the right under *Additional Settings*. Next, select the check box next to the *Legacy Proxy Types* to migrate.

To have the proxy migration task run continuously, deselect the check box next to each day of the week. To constrain the generation task to run within a certain period, select the check box next to the desired day of the week and the appropriate start time and end time.

Click **Save** at the top of the page when configuration is complete. Click **Start** in the *Task History* section to start the generation task.

Similar to proxy generation, you can configure proxy migration to run continuously or only within a specified period. You configure these settings in the second section on the right side of the screen. In the *Schedule* panel, a list of check boxes and time selectors are displayed next to each day of the week.

Transcode Service Configuration

You configure the Transcode service through the DIVAdirector web interface. Navigate to the **Transcode Service** configuration section under the **Admin, Service Settings, Transcode Service** section. You must start the service before continuing configuration. If the service is started but the status is showing as down in the configuration section, verify that configuration settings documented in the *Oracle Installation and Configuration Guide* are set correctly.

Note: FFmpeg and Vantage are supported for use with the transcode service.

Use the following procedure to configure the transcoder settings:

1. Set the transcoder implementation's *Host Address* and *Port*.
2. Define any *Metadata Action Descriptions*. These values store the descriptions of actions in a workflow that expose metadata variables that should be associated with a job.

3. Add any *Workflow Presets* required. These values store a named mapping to a transcoder implementation's internal workflow identifier. For Vantage, the *InternalId* is the workflow identifier. Typically, you will add at least one preset for creating proxies. You can add additional presets for alternate workflows. For example, if a Proxy Drop Folder is configured to automatically obtain thumbnails or metadata from dropped proxy files, then you can add those presets here.
4. Define an *Output Storage Location*. This value will form the base output path for the transcoded job. The remainder of the path will be formed by the *JobID* returned from the transcode service. For example, if the location path is `\\10.0.0.1\output`, and a *JobID* `6449d0db-2377-4e3d-a969-be09a742a63d` is returned from the transcode service, then the final output path for the transcoded file will be `\\10.0.0.1\output\6449d0db-2377-4e3d-a969-be09a742a63d`.

Starting and Stopping the Transcode Service Windows Services

Both Windows services installed with the Transcode Service should be set to start automatically. The two services display in the Windows Service Manager using the names *Oracle.Transcode.Api.Owin* and *Oracle.Transcode.TaskManager*.

You can manually control either of the services from the Windows Services Manager or using a Windows command line. Use the following command line options to control either of the services:

install

This option installs the service.

start

This option starts the service.

stop

This option stops the service.

restart

This option stops and then restarts the service.

uninstall

This option removes the service.

status

This option shows the current status of the service.

help

This option displays a help dialog.

For example, use the following command to start the API Service:

```
Oracle.Transcode.Api.Owin.exe start
```

Use the following command to stop and subsequently restart the Background Task Service:

```
Oracle.Transcode.TaskManager.exe restart
```

Configuration File Changes

The *Oracle.DIVAdirector.TaskManager* Windows Service configuration file (`Oracle.DIVAdirector.TaskManager.exe.config`) is located in the `C:\Program Files (x86)\DIVAdirector 5\TaskManager\` folder.

The configuration file has four main sections that need your attention as described below.

1. DIVA Enterprise Connect Endpoint Configuration

You must configure the following parameters for the DIVA Enterprise Connect endpoint:

AppName

This parameter is the name of the application to be registered in the WS API interface. Specifically, this is the value of the `appName` parameter passed to the `registerClient` method. This is required before interfacing with the WS API.

```
<add key="AppName" value="DIVAdirector"/>
```

ProcessId

This parameter identifies the process ID number used for registering the client application. Specifically, the value of the `processID` parameter passed to the `registerClient` method. This is required before interfacing with the API.

```
<add key="ProcessId" value="1234" />
```

LocationName

This parameter identifies the physical location where the computer running the client is located. Specifically, the value of the `locName` parameter passed to the `registerClient` method. This is required before interfacing with the WS API.

```
<add key="LocationName" value="location name" />
```

DIVArchiveApiUrl

This parameter identifies the WS API REST endpoint.

```
<add key="DIVArchiveApiUrl" value="https://DIVA-VM-105:9444/diva/service/rest/2.2/DIVArchiveWS_REST" />
```

ClientId

This parameter is the client id (user name) generated by the Key Generator script during the DWS installation.

```
<add key="ClientId" value="e3af4c10-e7ca-4143-970a-46bc0264a46f" />
```

ApiKey

This parameter is the API key (password) generated by the Key Generator script during the DWS installation.

```
<add key="ApiKey" value="kAkWTK3ObnE0mHheJAKP" />
```

DWSVersion

This parameter is the version of the API service that DIVAdirector is targeting.

```
<add key="DWSVersion" value="2.2"/>
```

Four settings require configuration in the `<appSettings>` section:

applicationName

This is the name of the application to be registered in the WS API interface. Specifically, this is the value of the *appName* parameter passed to the *registerClient* method. This is required before interfacing with the WS API.

```
<add key="applicationName" value="app name" />
```

locationName

This identifies the physical location where the computer running the client is located. Specifically, the value of the *locName* parameter passed to the *registerClient* method. This is required before interfacing with the WS API.

```
<add key="locationName" value="location name" />
```

processID

This identifies the process ID number used for registering the client application. Specifically, the value of the *processID* parameter passed to the *registerClient* method. This is required before interfacing with the WS API.

```
<add key="processId" value="1234" />
```

DIVArchiveApiUrl

This identifies the WS API REST endpoint. You can use any available port number for the endpoint.

```
<add key="DIVArchiveApiUrl"
value="http://10.80.106.57:9763/services/DIVArchiveWS_REST_2.1/" />
```

2. Transcoder Service Access Configuration

You must set the URL for the transcode service endpoint in the `<TranscodeSettingsConfigurationSection>` section.

```
<TranscoderClientSettings TranscoderApiUrl="http://localhost:9876/api/" />
```

3. Task and Task Interval Configuration

The following tasks are configured in the `<ScheduledTasks>` section and run by the Windows service. You cannot disable any of these tasks without losing functionality. However, you can tune an interval timer with the *IntervalInSeconds* parameter to achieve better performance.

HouseKeeperTask

This task automates system maintenance operations needed by DIVAdirector. These maintenance operations include both file system cleanup (removing old log files, purging system directories like `local archive`, `local proxy`, and so on), and database maintenance tasks.

TranscodeOnRestoreCompleteTask

This task polls the progress of a DIVArchive Restore request (through the DIVArchive Web Services API REST endpoint), and initiates a Transcode request upon completion. This task is also responsible for calling the Proxy Creation Service.

DIVArchiveSyncTask

This task controls synchronizing objects with DIVArchive.

UpdateRequestsStatusTask

This task is responsible for updating the status of a DIVArchive request.

CreateProxyOnRequestCompleteTask

This task is responsible for creating proxies in DIVAdirector by sending requests to the transcoding service when a DIVArchive request completes.

ProxyGenerationTask

This task is responsible for handling the automatic queuing of proxy generation tasks.

ProxiesMigrationTask

This task is responsible for handling the automatic migration of legacy proxies to newer formats.

CreateProxyOnJobCompleteTask

This task is responsible for creating proxies in DIVAdirector for transcode jobs not associated with a DIVArchive request.

LegacyStorageMigrationTask

This task governs the restructuring of the proxy storage locations after an upgrade from an earlier release. Users will not be able to log in to the system while the task is in progress.

Vantage Implementation

The Transcode Service can integrate with one or more Vantage servers through the Vantage web SDK. At a high level, configuration of a Vantage integration involves setting the IP address and port number of the Vantage SDK endpoint and mapping Vantage Workflow properties to Transcode Service preset values.

Vantage Stand-alone Integration

The most straightforward Vantage integration option is one where a single Vantage server generates all of the required artifacts (video file, thumbnail images, metadata) for a DIVAdirector proxy. To use this integration option, you can use the sample workflow installed with the Transcode Service (DefaultVideoProxy_Analysis). This option requires a Vantage Analysis license because it uses the Analyze and MediaInfo actions to extract the required metadata.

Configuring the Vantage Stand-alone Presets

Navigate to Admin>System>Service Settings>Transcoder Service>Transcoders

Task 1 Configure Transcoder Settings

1. Click the **red plus** button to create a new transcoder.
2. In Transcoder Settings, select **Vantage** for the type.
3. Give the transcoder a unique name.
4. Add additional descriptive text to the description field.
5. Adjust queue size if needed. This value will determine the number of simultaneous transcode jobs the transcoder can accept.
6. Select the **Enabled?** checkbox to activate this transcoder and allow it to be used in DIVAdirector workflows.
7. Set the IP address of the server hosting the Vantage SDK service.
8. Set the port used by the Vantage SDK service. On default installations, this will be port 8676.

Task 2 Define Presets

1. In the Presets panel, click **Add new record**.
2. Give the preset a name. This must be unique per transcoder, but the same preset name can be used by other transcoders.

You can configure a multiple transcoder setup by defining multiple transcoders with the same preset name. See "[Multiple Transcoders and Load Balancing](#)" on page 2-38.

3. Select the preset type:
 - **Video Proxy** — creates a proxy with automatic or manual workflow.
 - **Thumbnail Only** — extracts thumbnail images for EDLs (such as Shotlist page).
 - **Metadata Only** — extracts the required metadata fields for proxy generation. This is used for configuring split workflow setups. See "[Configuring Vantage Split Workflow](#)" on page 2-36.
 - **Thumbnail & Metadata** — extracts thumbnail images and metadata for use in drop folders configurations.
4. Set the Internal Id to match the Vantage Workflow Id of the corresponding workflow.
5. If you are using a Video proxy preset in a split workflow configuration (ex. Vanatage server without an Analysis license), then select the **Requires External Metadata** checkbox. See "[Configuring Vantage Split Workflow](#)" on page 2-36.
6. Enter any metadata action descriptions. This field is a comma-separated list of strings defining Vantage action descriptions that produce the metadata required for proxy creation. Required metadata fields are:
 - **OutputFileFullPath** — the fully qualified path of transcoded file.
 - **Video Framerate** — the frame rate of transcoded file.
 - **Content Duration** — the duration of transcoded file
 - **Header Timecode** — the timecode offset of first frame. This is only required if using a clip with a non-zero SOM.
7. Click **Insert**, and then **Save**.

Configuring Vantage Split Workflow

A Vantage split workflow configuration allows a Vantage server to be used for proxy file and thumbnail generation, while another transcoder is used for extracting the required metadata. This setup is achieved by configuring presets to indicate when one preset produces metadata and when another requires externally produced metadata.

Navigate to **Admin>System>Service Settings>Transcoder Service>Transcoders**.

Task 1 Configure Metadata Only Transcoder Settings

1. Click the **red plus** button to create a new transcoder.
2. In Transcoder Settings, select **Default Command line** for the type.
3. Give the transcoder a unique name.
4. Add additional descriptive text to the description field.

5. Adjust queue size if needed. This value will determine the number of simultaneous transcode jobs the transcoder can accept.
6. Select the **Enabled?** checkbox to activate this transcoder and allow it to be used in DIVAdirector workflows.

Task 2 Define Presets to Produce Required Metadata for Proxy Generation

1. In the Presets panel, click **Add new record**.
2. Give the preset a name. This must be unique per transcoder, but the same preset name can be used by other transcoders.
3. Select **Metadata Only** for the preset type.
4. In “exe path”, enter the fully qualified path to the executable (without parameters) to be used for extraction.

In a default setup this path is used:

```
C:\Program Files (x86)\Oracle Corporation\TranscodeService\Plugins\ffprobe.exe
```

5. In “exe args”, enter the arguments to pass to the executable entered above.

In a default setup, this value used is: `-i "{{input_filepath}}"`

Where the `{{input_filepath}}` string will be substituted with the fully qualified path of the input file when processing a job request.

6. Select the **Ignore StdError Output** checkbox if the exe will write output to std error that shouldn't be interpreted as an error.
7. Click **Update**, and then **Save**.

Task 3 Define a Vantage Video Proxy Preset Type that Requires Externally Generated Metadata

1. On the Vantage server, create or import a workflow that will create the proxy video and thumbnail (but doesn't extract required metadata).

An example is `DefaultVideoProxy_No_Metadata.xml`, installed by the Transcode Service in the installation directory:

```
C:\Program Files (x86)\Oracle Corporation\TranscodeService\SampleWorkflows\TranscoderSetupFiles\Vantage
```

2. Create a new preset record and select type **Video Proxy**.
3. Map the Internal Id field to the corresponding Vantage workflow Id.
4. Select the **Requires External Metadata** checkbox.

When this option is selected and a job is submitted with this preset, the Transcode Service will search for any preset of type “Metadata Only” in any enabled transcoder. If no such preset is available, then the job will fail. If a “Metadata Only” is available, then the metadata extraction task will be queued first. If the metadata extraction task succeeds, then the processing of the original preset will continue.

5. Set “Metadata action descriptions” for the metadata output by Vantage. Since this is a split workflow and most of the metadata is produced by an external preset, typically the only value here will be the action description that produces the fully qualified path of the output file (`MD_OUTPUT_PATH` for the sample workflow).
6. Click **Update**, and then **Save**.

Multiple Transcoders and Load Balancing

With DIVAdirector 5.4.1, you can distribute transcoding tasks among multiple transcoder implementations. You configure this by setting up multiple transcoders with a shared preset name. An example scenario would be configuring load balancing for automatic proxy generation tasks across servers: Vantage1 and Vantage2.

With the following configuration, any automatic proxy generation tasks for the configured category will be distributed between Vantage 1 and Vantage 2:

Note: The preset name does not have to be “shared”, but it must be the same for both servers.

1. Follow the steps in "[Configuring the Vantage Stand-alone Presets](#)" on page 2-35 to configure the Vantage 1 server.
2. Create a Video Proxy preset with name “shared” in Vantage 1.
3. Save Vantage 1 configuration.
4. Follow the steps in "[Configuring the Vantage Stand-alone Presets](#)" on page 2-35 to configure the Vantage 2 server.
5. Create a Video Proxy preset with name “shared” in Vantage 2.
6. Save Vantage 2 configuration.
7. Navigate to **Admin>System>Proxies>Proxy Generation**.
8. Create a new Category Filter with workflow name set to “shared”.

Command Line Transcoder - Custom Script Integration

You can directly integrate Command line transcoders, like FFmpeg, with the Transcode Service by configuring an implementation to directly invoke the command line executable.

There are several drawbacks to this approach. First, the transcoder must be able to produce all of the required proxy artifacts: video file, thumbnail images, and metadata – with a single command. Second, the artifacts will need to conform to a specific format. For example, the thumbnail images will need to be named in a format with the SOM-based SMPTE timecode appended to the file name. Because it can be difficult to produce all of these artifacts with a single command in the required format, another integration option is available.

Instead of directly invoking the command-line transcoder, you can configure the Transcode Service to call a custom script to produce the required proxy artifacts. With this option, the script can call multiple commands.

Sample Powershell scripts are installed with the Transcode Service in the directory: C:\Program Files (x86)\Oracle Corporation\TranscodeService\SampleWorkflows\TranscoderSetupFiles\Custom for default configurations. The scripts are not limited to Powershell. You can use other scripting engines like Python.

Configuring the Command Line Transcoder Script

Navigate to **Admin>System>Service Settings>Transcoder Service>Transcoders**.

Task 1 Configure Custom Command Transcoder Settings

1. Click the **red plus** button to create a new transcoder.

2. In Transcoder Settings, select **Custom Command line** for the type.
3. Give the transcoder a unique name.
4. Add additional descriptive text to the description field.
5. Adjust queue size if needed. This value will determine the number of simultaneous transcode jobs the transcoder can accept.
6. Select the **Enabled?** checkbox to activate this transcoder and allow it to be used in DIVAdirector workflows.

Task 2 Define Custom Command Video Proxy Preset

1. In the Presets panel, click **Add new record** button.
2. Give the preset a name. This must be unique per transcoder, but the same preset name can be used by other transcoders.
3. Select **Video Proxy** for the preset type.
4. In “exe path”, enter the path of the scripting engine that will be used. For default installations, this is: Powershell.exe.
5. In “exe args”, enter the arguments to pass to the executable entered above. In a default setup, this is:

```
-ExecutionPolicy ByPass -File "C:\Program Files (x86)\Oracle Corporation\TranscodeService\SampleWorkflows\TranscoderSetupFiles\Custom\ffmpeg_proxy.ps1" "{{input_filepath}}" "{{output_basepath}}"
"{{output_filename}}.mp4"
```

6. Select the **Ignore StdError Output** checkbox if the exe will write output to std error that shouldn't be interpreted as an error.
7. Click **Update**, and then **Save**.

Custom Script Parameters

The following parameters, enclosed in double curly braces, will be substituted at runtime.

- `{{input_filepath}}` — Fully-qualified path of the input file to the custom script.
- `{{output_basepath}}` — Fully-qualified base path for storing the proxy artifacts. This is a temporary subdirectory stored under the staging location. Files output by the transcoder will be stored here until they are transferred by the DIVAdirector Task Manager service to the proxy storage location.
- `{{output_filename}}` — Filename (without extension) of the transcoded proxy file.

The custom script will need to use the interpolated values for placing the artifacts in the correct location. The following are example parameters from the default Powershell script installed with Transcode Service:

```
Param(
    [string]$input_filepath,
    [string]$output_basepath,
    [string]$output_filename
)
```

With the following parameter values:

- `$output_basepath` — `\\Staging\4d769747-adde-456e-8350-125360241daf`

- `$output_filename` — `outputfilename`
- `$input_filepath` — `\\RestoreLocation\inputfile.mxf`

The custom script would need to create a proxy file named `$output_filename` under the `$output_basepath` directory.

For example:

```
\\Staging\4d769747-adde-456e-8350-125360241daf\outputfilename.mp4
```

You will need to place thumbnail images in a subdirectory named `Keyframes` under `$output_basepath`. The filename format of the images should contain the SOM based SMPTE timecode appended after an underscore character.

For example, for thumbnails extracted every 10 sec from a source clip with a 01:00:00:00 SOM.

```
\\Staging\4d769747-adde-456e-8350-125360241daf\Keyframes\prefix_01001000.jpg
```

```
...
```

```
\\Staging\4d769747-adde-456e-8350-125360241daf\Keyframes\prefix_01004000.jpg
```

You should store metadata in a JSON formatted string in a file named `metadata.json` under the `$output_basepath` directory.

For example: `\\Staging\4d769747-adde-456e-8350-125360241daf\metadata.json`.

Required keys are “content duration” and “video framerate”.

Logging Configuration

Now that the storage is configured for the system, you are going to configure the log files. There are three important sets of log files used in DIVAdirector:

- WWW Log Files
- Task Manager Log Files
- API Log Files

All DIVAdirector logs aggregate on the same UDP port (7071 by default) and can be monitored by Log4Net compliant logging applications (for example, Log2Console) to provide live system monitoring. However, many of these logging applications are extremely resource intensive and should not be left running in the background.

The xml format for logging configuration will be the same for every type of log as follows:

```
<log4net>
  <appender name="UdpAppender" type="log4net.Appender.UdpAppender">
    <remoteAddress value="127.0.0.1" />
    <remotePort value="7071" />
    <layout type="log4net.Layout.XmlLayoutSchemaLog4j" />
  </appender>

  <appender name="RollingFileAppender"
type="log4net.Appender.RollingFileAppender">
    <file value="logs/logfile.log" />
    <appendToFile value="true" />
    <maximumFileSize value="5MB" />
    <maxSizeRollBackups value="5" />
    <layout type="log4net.Layout.XmlLayoutSchemaLog4j" />
  </appender>

</root>
```

```

    <level value="DEBUG" />
    <appender-ref ref="RollingFileAppender" />
    <appender-ref ref="UdpAppender" />
  </root>
</log4net>

```

The only values that should be adjusted are the following:

maximumFileSize

This parameter is the maximum size a log file will attain before rolling over to another log. If you find that having larger individual log files better suits your needs, then adjust this value.

maxSizeRollBackups

This parameter is the maximum number of rolled log files that can be produced per day. Any additional logging for the day will be ignored. If you find that too many log entries are being created per day, then adjust this value.

level

This value refers to the detail of the logs. Valid values are the following:

ALL

At this level all logs are collected including Trace level logging. Only use this option at the request of Oracle Support.

DEBUG

Debug logging is quite extensive and can degrade performance in a particularly busy system. *Only use this option at the request of Oracle Support.*

INFO

At this level only informational messages, warnings and errors are collected. *Oracle recommends using this as your production system setting.*

WARN

At this level only warnings and errors are collected.

ERROR

At this level you will only see errors appear in the logs.

Note: The Oracle DIVA Enterprise Connect logs, IIS logs and PostgreSQL logs may also be useful when troubleshooting potential problems. *See the respective application documentation for advice on setting logging levels and location.*

Oracle DIVAdirector WWW Logging Configuration

Caution: Changing the `Web.Config` file should only be done when the site is offline. Making changes when the site is live will force the site to reset, logging out all users.

The WWW logs contain information regarding any user interactions with the Web Interface and secondary interactions with various connected services, such as Oracle DIVA Enterprise Connect. The default setting for these logs is enabled, and they

provide a good starting point for investigating any operational, or configuration, errors.

The configuration for these log files is located in the C:\Program Files (x86)\DIVAdirector 5\www\Web.Config file.

Oracle DIVAdirector Task Manager Logging Configuration

The Task Manager logs contain information regarding scheduled tasks, including Drop Folder operations, synchronization, request updating, and housekeeping, among others (see [Task Manager and DIVAdirector API Windows Services](#) for more information).

The configuration for these log files is located in the C:\Program Files (x86)\DIVAdirector 5\Task Manager\log4net.config file.

Note: After changing the any parameters in the configuration file you must restart the Oracle.DIVAdirector.TaskManager service. The restart triggers an automatic HouseKeeping task, and therefore Oracle recommends restarting during non-business hours (if possible).

Oracle DIVAdirector API Logging Configuration

The API logs contain information regarding user log in, and any interactions with the Oracle Client Uploader.

The configuration for these log files is located in the C:\Program Files (x86)\DIVAdirector 5\API\log4net.config file.

Note: After changing the any parameters in the configuration file you must restart the Oracle.DIVAdirector.Api service.

Next you will configure search parameters.

Search Configuration

The following sections include detailed information for managing metadata. Metadata is used in system wide searches on the DIVAdirector and DIVArchive systems to locate a specific file, category of files, objects, or video clips. These roles are set for the group and apply to all members of the group.

Object Metadata

Object metadata is a set of search terms that belong to an object. Each object has its own predefined set of metadata. Metadata is imported from DIVArchive (OBJECT_NAME, OBJECT_CATEGORY, ARCHIVE_DATE, and so on).

The Object Metadata screen is accessible from the **Admin, Users, Metadata** screen. The following functions are available from the **Object Metadata** screen:

- You click **Add** on the top right side of the screen to add new metadata for objects in DIVAdirector.
- You select the metadata type to be deleted in the list, and then click **Delete** on the top right side of the screen to delete an existing metadata type.

- You click the **Pencil** icon at the beginning of the row for the metadata to be edited to edit a metadata type.

Data Types

DIVAdirector supports various data types for metadata field definitions and associated presentation controls. When you select a specific data type additional parameters are presented to the user.

The following are the valid metadata types:

String

Any character string; restricted to 1 - 100000 characters in length. The *String* data type can be represented using an **EditBox**, **TextBox**, or **SelectBox** control (refer to [DIVAdirector Presentation Controls](#)).

Number

Any integer numeric value. The *Number* data type can be represented using an **EditBox** or **CheckBox** control.

Decimal

Any numeric value - including decimals. The *Decimal* data type can be represented using an **EditBox** or **CheckBox** control.

Date

The *Date* field can be represented using an **EditBox**, **SelectBox**, or **Calendar** control.

Time

The *Time* field can be represented using an **EditBox** or **SelectBox** control.

Binary File

A fixed representation file of arbitrary internal format which is represented using a **FileSelect** control.

SAMMA Graph

A graphical representation of metadata that originated from Oracle SAMMA solo. The graph can represent the entire object or just a portion of the object.

SAMMA Thumbnail

A representation of thumbnails of frames that match the portion of the object represented by the SAMMA Graph.

Quality Control Report

Used for Quality Control reporting. Options include the following:

- Report Type
- Selected (selected or deselected)
- Data file extension
- Report file extension

DIVAdirector Presentation Controls

Most metadata field data types have multiple ways of displaying data and some are restricted to using particular controls. The following are descriptions of the controls used to display the metadata fields:

EditBox

A single line text entry control that allows users to edit its value.

TextBox

A general multi-line text editing control.

Select

Allows users to select a value from the supplied list of unique values.

CheckBox

Allows users to select an option by selecting the appropriate check box.

Calendar

Allows users to browse through a graphical calendar and select the appropriate date. This format is used only for the *Date* data type.

FileSelect

A special composite control comprised of an **Upload** button, and link to an existing binary file. This format is used only for the *Binary File* data type.

SAMMA Graph

This control is only used for the *SAMMA Graph* data type and shows a graphical representation of Oracle SAMMASolo generated metadata.

SAMMA Thumbnail

This is only used for the *SAMMA Thumbnail* data type to provide thumbnail representations of frames that match the portion of the objects represented by a *SAMMA Graph* control.

Predefined Metadata Display Columns

The metadata display screen is arranged in a tabular format. The columns in the table are predefined and described as follows:

ID

DIVAdirector defined unique identifier for the object.

Name

DIVArchive system defined object name used as a unique identifier with the category.

Category

DIVArchive system defined object category used with the name.

Date

The date when the object was archived to the DIVArchive system.

Comments

A comment text field that contains comments added during the object's creation.

Source

The original source of the file from which the object was created.

Active

The current object status that determines whether the object exists.

Virtual

The flag defining whether the object is virtual (YES or NO).

Site

The archive system, or systems, that an object is on.

File Size

The total size on disk for an object.

Tape VSN

The tape barcodes that contain instances of an object.

First you will add new metadata entries.

Adding a Metadata Entry

Use the following procedure to add a new metadata entry to the Metadata Manager:

1. Navigate to **Admin, Metadata** in the navigation menu on the left side of the screen.
2. Click **Add** on the top right side of the screen.
3. Enter the information in the resulting dialog box.
4. Click the **Check** icon on the lower left side of the screen to add the new entry, or to click the **X** icon on the lower left side of the screen to cancel the addition.
5. Repeat the previous steps for each metadata entry you must add to the system.

When a metadata type is selected from the list additional parameter fields are displayed that are specific to the type selected. Each metadata entry has the following parameters:

Title

The *Title* field is the Metadata column name displayed in the user interface. The title can be any unicode text with maximum length of 32 characters.

Type

The *Type* field determines the entry's data type and is defined automatically when selected from the *Type* list. For example, if the type of the Metadata column is `DATETIME` in the database, then one of the two types can be selected from the list, **DATE** or **TIME**.

Format

The type of the presentation control used.

File Mask

If you select the **Binary File** type, the edit field will be displayed instead of the column length. Only files with this mask can be selected to be uploaded using the *Object Metadata* area of the **Shot List** screen. Multiple masks can be set and separated by a semicolon. For example, you can enter `*.txt; *.log` and any spaces will be removed when saved (in this case).

Description

This is the description of the column displayed in the Tooltip when the user hovers over the column title in the *Query Results*, the *Work Bin* tables on the **Search** screen, and the *Asset Metadata* area on the **Shot List** screen. The description can be any unicode text and has a maximum length of 240 characters.

Display Options (Flags)

One or more of the following:

- **Hidden**

- **Read Only**
- **Display in Search Results**
- **Display in Tooltips**

In addition to the above, a SAMMA Graph metadata column type requires the following parameters:

Y Axis Label

This specifies the name of the Y Axis for the SAMMA Graph.

Graph Tags

Specifies the type of information to be displayed on the SAMMA Graph. Click + on the **Field Tag** button to add each tag and specify a color. Predefined tags are available in the *Choose Type* list or by clicking on the default type displayed under the *Field Tag*. For example, using the *Choose Type* list and selecting the type as **Video** results in three field tags being created automatically:

- **Luminance Average**
- **Chroma U Average**
- **Chroma V Average**

Next you will configure quality control report metadata.

Add Quality Control Metadata

You add Quality Control report metadata to the system's search functions using the following procedure:

1. Open the *Metadata Column Manager* on the **Admin, Metadata** screen.
2. Click **Add** on the top right side of the screen.
3. Enter a name for the metadata in the *Title* field.
4. Select **qc report** from the *Type* list.
5. Select **QC Report** from the *Format* list.
6. Select which reports should be visible using the check boxes next to each type of report.
7. Enter the data file extension (usually `xml`) for each visible report in the *Data Extension* field.
8. Enter the report file extension (`xml` or `pdf`) in the *Report File Extension* field.
If an XML file for data and PDF file for viewing are both available, set the *Report File Extension* to `pdf`. In most cases, it can remain set to the default value (`xml`).
9. Enter a description in the *Description* field.
10. Select the **Hidden (Hid)** check box if you want the report hidden from users; otherwise, leave it deselected.
11. Click the **Check** icon on the lower left side of the screen to save the new report column, or click the red **X** icon to cancel the addition.

Next you will configure metadata access for the group.

Metadata Filters

Metadata filters authorize and restrict user access to various metadata fields. You configure the filters on a per group (not per user) basis on the **Permissions (Metadata)** tab in the **Groups** screen. Users can only view the metadata fields that their group has access permissions to.

The metadata filters are applied only within **Queries**, **Edit Metadata**, and **Shot List** screens. Each field can be made accessible, inaccessible, and available or unavailable, for publishing (refer to the *Oracle DIVAdirector User's Guide* for more information on publishing).

Next you will configure metadata publishing settings.

Metadata Publish Settings

DIVAdirector can publish restored video clips to editing software. A destination configured in DIVArchive must point to the editing software location that is receiving the restored video clips and their metadata to use the publishing functions. This setting must be selected as the location for publishing in the *DIVArchive Destination* list on the **Metadata Publish Settings** tab on the **Groups** screen.

The FTP network protocol is used for DIVAdirector's *Publish Metadata* feature and must be configured in the FTP area of the screen. Publishing clips to editing software requires sending the video clip's metadata as an XML file.

Metadata fields to be included in the XML file are selectable in the **Metadata** area of the screen. The available fields are determined by the settings configured in the *Metadata Permissions Filter*.

1. Select the available metadata fields to include in the XML file using the check box to the right of each field. A selected check box will include the field in the XML file and a deselected check box will not be included.
2. Enter the FTP server's *Host*, *Username*, *Password* and *Port* number in the designated fields. The port number can be entered manually or you can use the up and down arrows to the right of the port field to raise or lower the displayed number. The default FTP port (25) will be used if the port field is left empty.
3. Select the destination from the *DIVArchive Destination* list.
4. Click **Save** on the top right side of the screen to save the settings.

Next you will configure quality control reports.

Automated Backup Configuration

You configure automated backup operations by identifying your desired schedule, and then selecting the check box to make the scheduled task active. The schedule can be set to run on a weekly or monthly basis.

Caution: Although you can delete scheduled tasks in the Windows Explorer, *do not* use this method to remove the task. If the task was accidentally deleted in the Scheduled Tasks, the Windows registry key named HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Front Porch Digital Inc.\DIVAdirector\DB\Backup must be removed, enabling DIVAdirector to be able to configure further scheduled backups correctly. *If you require assistance or are not comfortable editing the Windows registry contact Oracle Support.*

Use the following procedure to configure your automated backups:

1. Navigate to **Admin, Backup, Schedule** on the navigation tree on the left side of the screen.
2. Either enter the time to begin the backup directly in the *Start Time* field, or use the clock icon to the right of the *Start Time* field to display a selectable time menu called the *Time Picker*.

The *Start Time* field denotes the time when the backup should start and must be in 24 hour format using standard hh:mm notation where:

- hh = hours (0 - 23)
- mm = minutes (0 - 59)

3. Use the *Occurrence* list to select either a weekly or monthly backup frequency.

If the *Occurrence* is set to **Weekly**, you can assign the days of the week when the backup should be performed by selecting the check box to the left of each day desired.

If the *Occurrence* is set to **Monthly**, you can set a day of the month (by date) when the backup should be performed by selecting the day of the month from the *Days* list.

4. Select the destination folder for the backup snapshot files in the *Directory* field.

The root location is mapped to the virtual folder named `DIVAdirector Database Backup Storage`. Select the backup destination using the navigation provided in, or above, the *Directory* area on the right side of the screen.

5. Click **Save** on the top right side of the screen to apply the settings. When the changes are saved successfully, a confirmation message is displayed.

The DIVAdirector scheduled backup task that was created is now available (named `At1`). You can confirm correctness in the Windows Task Scheduler. Additional backup tasks will be numbered sequentially (for example, `At2`, `At3`, `At4`, and so on).

Your initial configuration of DIVAdirector is now complete. In the next chapter you will find daily tasks that you use to keep DIVAdirector running.

Quality Control (QC) Report Configuration

DIVAdirector supports integration with QC Reports from Venera Rapid, Venera Pulsar, Tektronix Cerify, and Interra Baton. Report files should be placed in the path under the IIS DIVAdirector 5 Root Folder:

```
DIVAdirector QC Report\{Report Name}\{Category}\{Object Name}\{Object Name}.xml
```

For example:

```
DIVAdirector QC Report\Venera Rapid\WMV\AUTO_20120615_031030\AUTO_20120615_031030.xml
```

First you will create a folder for the QC reports, then you will place all reports in the folder you create.

QC Report File Placement

Use the following procedure to create a folder for the QC Reports. After reports are created you will place the reports in the appropriate folder.

1. Open IIS and navigate to the **DIVAdirector QC Report** virtual directory under the **DIVAdirector 5** menu item.
2. Right-click the **DIVAdirector QC Report** folder, and then select **Explore** from the context menu.
3. Create a new folder with a specific category (for example, *Venera Rapid* or *Venera Pulsar*) for the files under the report type folder.
4. Create a new folder using the report name (for example, *AUTO_20120615_031030*).
5. Place the QC Report XML files in the newly created folder. Other report files (for example, PDF files) can be placed in the same location.

Next you will configure automated system backups.

DIVAdirector Daily Operations

You must monitor DIVAdirector daily to insure proper operation, storage capacities, orphaned files, user interaction, successful backups, and general system health. If you discover any anomalies that you are uncertain of or if you are unsure of how to handle them, contact Oracle Support for assistance.

This chapter describes your daily operations routine and includes the following information:

- [Checking Available Storage Capacity](#)
- [Checking for Orphaned Files](#)
- [Checking Audit Trails](#)
- [Checking for Successful Backup Completion](#)

Checking Available Storage Capacity

In your initial DIVAdirector configuration you identified system storage locations and the limits for each location. Storage locations will fill up over time during normal use. You must check the remaining available space for each location daily. If a storage location is reaching its limit, you must either migrate some (or all) of the data to another location (for proxy data see [Proxy Migration](#)) or configure a new location (see [Source/Destination Configuration](#)).

Use the following procedure to check your storage locations and remaining available space:

1. Navigate to the *Storage Location Configuration* section under **Admin, System, Storage Locations**.

2. Check each location's *State* to identify the current storage location status.

If the location's state is something other than operational (and you didn't set it that way), you must identify why it is in the current state, and if necessary, resolve the issue. You use the server logs and Drop Folder logs to help identify issues. If you are unable to resolve the issue and need further assistance contact Oracle Support.

3. Check the *Used* and *Available* columns to identify how much of the storage space is filled and how much is left available (respectively) for each location. You will need to decide if additional space is required, if data must be migrated to another location, or if the location is fine the way it is.
4. If you must add a new storage location refer to [Source/Destination Configuration](#).
5. If you must adjust the storage space limits refer to [Configuring the Proxy Storage Location](#).

6. If you must migrate data to another storage location see [Proxy Migration](#) for information.

Next you will check for orphaned files.

Checking for Orphaned Files

Throughout daily user interaction with DIVAdirector, you will occasionally get some orphaned files. Orphaned files are files that were placed in a Drop Folder and had the wrong format, had different encapsulation than configured for the folder, or they do not exist in the database. The system identifies the files as *unrecognized* and moves them to a special *Orphan* folder. You identified the *Orphan* folder during your initial configuration (see [Drop Folder Configuration](#)).

Use the following procedure to locate and act on orphaned files:

1. Open Windows File Explorer.
2. Navigate to the *Orphan* folder you configured for your first Drop Folder.
3. Identify the contents of each file inside the folder.
4. When you identify what the file is, decide whether to:
 - Repair whatever caused the file to be placed in the orphan folder, and then re-drop it into the Drop Folder for re-processing.
 - Move the file to another storage location.
 - Delete the file.

Determine the action you take on each file according to your internal organizational policy and the importance of the file.

Next you will check the user interaction with audit trails.

Checking Audit Trails

Audit trails are checked to review system and user activity formed on specific objects. This is useful for general system overview, and to determine if errors occurred while a user was trying to perform an action on a specific object.

The **Audit Trail** screen displays user interactions with the DIVAdirector system. You can filter the display by *Action*, *User*, *Time (From and To)*, *Object Name*, and *Object Category* using the options on the right side of the screen. The *Object Name* and *Object Category* fields in the filter can contain partial words.

For example, use the following procedure if you are searching specifically for actions performed by a user in the Marketing Department on an object named *MySportsVideos* and having the object category *MOV*:

1. Enter *Mark* in the *Organization* field, and select the *Organization* check box.
2. Enter *My* in the *Object Name* field, and select the *Object Name* check box.
3. Enter *MO* in the *Object Category* field, and select the *Object Category* check box.
4. Click **Apply Filter** on the bottom right side of the screen to locate the object.

This procedure will locate the object if it exists in the audit trail.

Clicking **Export** on the top right side of the screen will export the filtered (or unfiltered) audit trail to a file that you can use for tracking general system use or errors.

Checking for Successful Backup Completion

System backups are necessary and extremely important for disaster recovery. You must confirm that the backups you created during initial configuration are completing successfully and to the proper storage location. You cannot restore a corrupt backup file so you must check them daily.

Use the following procedure to check the backup files:

1. Open Windows Explorer.
2. Navigate to the storage location you designated in the initial system configuration. See [Automated Backup Configuration](#) if you need a reminder of where you set the backup storage location.
3. Check the creation date and time of the latest file in the folder. Confirm that the date and time match the backup schedule.
4. Check the system log files for errors related to the backup job. See [Checking Log Files](#) for the procedure to use.

If a corrupt or unsuccessful backup is discovered, use the procedure described in [Performing a Manual Backup](#) to attempt a manual system backup before attempting to troubleshoot any issues.

In the next chapter you will find system maintenance tasks that you must use occasionally.

System Management

You must perform occasional system maintenance tasks on DIVAdirector. The tasks are completed on an *as needed* basis and include database synchronization editing, storage management, data and resource management, account management, and so on.

This chapter describes occasional maintenance and includes the following information:

- Database Synchronization Management
- Proxy Storage Management
- User Data and Resource Management
- Account Management
- Search Management
- Session Management
- Administrator's Message
- Configuration for ShuttlePro V2 or ShuttleXpress Control Pads

Database Synchronization Management

You added database synchronization filters in your initial DIVAdirector configuration (see [Synchronization Filtering](#)). You can update or remove existing filters as necessary. You can edit, enable, disable, or remove filters from the synchronization filter list.

Use the following procedure to edit an existing synchronization filter:

1. Select the filter and click the **Pencil** icon to enter the **Edit** screen.
2. You can now make any necessary changes to the filter
3. Click the **Check** icon to save your changes.

Use the following procedure to enable or disable a synchronization filter:

1. Select the filter and click the **Pencil** icon to enter the **Edit** screen.
2. Either select the **Enable** check box to enable the filter, or deselect the check box to disable the filter.
3. Click the **Check** icon to save your changes.

Use the following procedure to remove a synchronization filter from the filter list:

1. Locate the filter you want to remove in the list.

2. Click the red X icon on the right side of the filter entry.
3. The filter is now removed from the list.

Proxy Storage Management

You will check storage capacities during your daily system monitoring. Eventually you will have to add, reconfigure, remove storage locations, (see [Configuring the Proxy Storage Location](#)) or rearrange storage search priority. At times you may have to migrate data from one storage location to another for various reasons, such as replacing a storage location, making more storage space available, and so on.

You will also need to check for the Legacy Storage Migration progress when you upgrade from a DIVAdirector 5.3 and below. To find the migration progress and a checkbox to enable the storage migration, go to Admin, System, Storage Locations. These are only visible if there are eligible proxies to migrate.

User Data and Resource Management

Users have the ability to make their private data public so other users can see it including queries, *Work Bins* and *Shot Lists*. After a user makes a resource public, you are the only user who can change it back to private again. If a user requests a status change for one of their resources or if you suspect unauthorized access to data, you can make public resources private as appropriate for the situation.

Making a Public Resource Private

Caution: If you select the **Make Private** menu item, the selected resources become private without additional confirmation.

You manage public resources such as queries, *Work Bins* and *Shot Lists* on the **Admin, System, Public Resources** screen. Any item made public by a user can only be made private again by you from this page. Information about public resources such as resource name, type, user who created the resource, creation time, and time when resource was made public, is displayed on this screen. When you delete a user who owns one or more public resources from the system, the `admin` user automatically becomes the owner of those public resources.

You can select one or more resources to make private and use the following procedure to change the resource from public to private:

1. To select multiple items simultaneously, press (and hold) the **Control** key, and click (once) on each resource with the mouse.
2. To select a range of resources, press (and hold) the **Shift** key, click the first, and then the last resource in the range. All items in the range will be highlighted.
3. Right-click the selection and select the **Make Private** context menu item to make the selected resources private.

Account Management

During normal operations you will eventually have to manage organization, group and user accounts. The following sections cover modifying and removing accounts. To add new accounts see [Account Configuration](#).

Managing Organizations

Typically an organization will not need modification or deletion. However, there are instances when a company reorganization may require you to add, change, or delete an organization. See [Adding an Organization](#) for instructions on adding organizations.

Modifying an Existing Organization

Use the following procedure to modify an existing organization:

Caution: Changes cannot be reset after they are saved. To make additional changes or corrections after saving modifications you must go through the organization modification procedure again, and then save the changes again.

1. Navigate to the **Admin, Users, Organizations** screen.
2. Select the organization to modify from the *Organization* list.
3. Modify the organization's properties as required.
4. Click **Save** on the top right side of the screen to apply the changes.

Deleting an Organization

Use the following procedure to delete an existing organization:

1. Navigate to the **Admin, Users, Organizations** screen.
2. Select the organization to delete from the *Organization* list.
3. After you select the organization, click **Delete** on the top right side of the screen.
4. Click **OK** in the resulting dialog box to confirm the deletion.

Managing Groups

Eventually you will have to add, modify, or delete groups during normal operations. Modifications could include changing user roles within the group, changing the group name, changing content filters, and so on. See [Adding a Group](#) for instructions on adding groups.

Modifying an Existing Group

Use the following procedure to modify an existing group:

1. Navigate to the **Admin, Users, Groups** screen.
2. Select the group name to be modified from the *Group* list.
3. As necessary, modify the group name in the *Group Name* field, the group permissions in the *Privileges* area, and the filters in the *Content Filter* area. Content filters are discussed in [Content Filters](#).
4. Click **Save** on the top right side of the screen to apply the changes.

Deleting an Existing Group

You are a member of the *SystemAdmins* group. You, and other users authorized by you, are members of the *Admin* group. You have full control of the system. Your account must always be available and therefore these two groups can never be deleted. If

deletion of these groups is attempted a warning message is displayed. *You should immediately check the security of the system.*

A group cannot be deleted unless it has no active members. If you attempt to delete a group with active members an error is displayed notifying you that there are active users in the group.

Use the following procedure to delete an existing group with no active users:

1. Navigate to the **Admin, Users, Groups** screen.
2. Select the group name to delete from the *Group* list.
3. Click **Delete** on the top right side of the screen.
4. Click **OK** in the resulting dialog box to confirm the deletion.

Managing User Accounts

During normal operations you will have to add, modify, or delete user accounts. This includes removing users who no longer require access to the system, employees who are no longer with the company, users who change departments (groups or organizations), and so on. User account modification includes changing email addresses, resetting passwords (if they forgot their password), changing user mailing addresses, and so on. See [Adding a User](#) for instruction on adding users.

Modifying an Existing User

Use the following procedure to modify an existing user account:

Caution: Changes cannot be reset after they are saved. To make additional changes or corrections after saving modifications, you must go through the user modification procedure again, and then save the changes again.

1. Navigate to the **Admin, Users, User** screen.
2. Select the user to be modified from the *User* list. The fields will either be filled in or empty depending upon the information previously entered when the user was created or last modified.
3. Modify the user's properties as required.
4. Click **Save** on the top right side of the screen to apply the changes.

Deleting a User

Use the following procedure to delete an existing user. Deleted users are not removed from the database and can be restored if deleted by mistake. To restore a deleted user contact Oracle Support for assistance. *The last user in the SystemAdmins group can never be deleted.*

1. Navigate to the **Admin, Users, User** screen.
2. Select the user account to be removed from the *User* list.
3. To remove the user click **Delete** on the top right side of the screen.

Search Management

You can add, update, or delete search metadata at any time. You added search metadata, defined content filters, and assigned metadata publishing roles during the initial system configuration. All modification and deletion of metadata entries occur on the **Admin, Metadata** screen. See [Adding a Metadata Entry](#) for instructions on adding search metadata.

Metadata Column Manager

The **Admin, Metadata** screen contains a table with metadata entries for both base and object metadata. Each row is a different metadata entry called a *Metadata Column* and displays the entry's parameters in the appropriate table column.

You add, remove, edit, and reorder Metadata Columns for on-screen display in the *Metadata Column Manager* table. Certain rows, such as the parameters from DIVArchive and Proxy Metadata, are predefined, will be always present in the table, and cannot be deleted.

You can change the order of the entries by dragging and dropping the row to another position to complete the repositioning.

Check boxes display the state of each entry, and you select or deselect the check boxes to enable or disable the different states.

Hid

Hidden - when selected the entry will not appear on the Metadata screen.

R/O

Read Only - when selected the entry will appear in the Metadata screen but cannot be modified.

SR

Search Results - when selected the entry will appear in the *Search Results List* view mode.

TT

Tooltip - when selected the entry will appear in the Tooltips.

Editing a Metadata Entry

Use the following procedure to edit a Metadata Column:

1. Navigate to the **Admin, Metadata** screen.
2. Locate the metadata entry to edit.
3. Click the **Pencil** icon in the first table column of the entry row.

The selected row is highlighted in the table and all parameters of the selected entry are displayed for editing.

4. When you are finished editing the entry, click the **Check** icon to save the changes or click the **X** icon to cancel the changes.

Deleting a Metadata Entry

Use the following procedure to delete a metadata entry:

1. Navigate to the **Admin, Metadata** screen.

2. Locate the metadata entry to delete.
3. Select the entry's row.
4. Click **Delete** on the top right side of the screen.
5. Click **OK** in the confirmation dialog box to delete the entry.

Session Management

The Session Management screen displays information about which users are currently online and which users are not logged in (offline). Each user can log in from only one location (browser session) at a time. User log in sessions have an inactivity timeout of one hour.

Currently logged in users can only see other logged in users and logged off statuses if the user's group visibility allows access to this function. For example, if the current user belongs to a group that does not have visibility of other groups, then only users within the same group are visible on the **Session Management** screen. The only exception is that users in the *SystemAdmins* group can always see all other users.

Use the following procedure to monitor user sessions, sort the table rows, and log off online users (if necessary):

1. Navigate to the **Admin, Session Management** screen.
Online users are displayed at the top of the screen and offline users at the bottom of the screen.
2. For display purposes, you can click the table header columns to sort the rows.
3. To log the user off from the system, right-click an online user and then select **Sign out user** from the context menu.

Administrator's Message

The **Message** screen allows (only) you to add, change, or delete a message displayed to all users of the system when they log in. There are three types of the messages:

- Announcement (this is the default)
- Warning
- Alert

Use the following procedure to add or update the system message:

1. Navigate to the **Admin, Users, Messages** screen.
2. Select the type of message from the *Type* list.
3. Enter the message text in the *Message* field.
4. Click **Save** on the top right side of the screen to save the message.

Configuration for ShuttlePro V2 or ShuttleXpress Control Pads

You install and configure Contour's control pad on your user's client computer. The ShuttlePro V2 or ShuttleXpress Control Pads are set up and configured by running the installer program supplied with the software and using the default selections.

When installation is complete, copy the Shuttle configuration file for the appropriate operating systems:

Windows 7

Copy C:\Program Files (x86)\DIVAdirector 5\Support\etc\Pref file - Windows\SDIshuttle.pref to C:\Program Data\Contour Design.

Note: Windows requires privileges to show hidden files in the Folder Settings to see the path.

macOS

Copy C:\Program Files (x86)\DIVAdirector 5\Support\etc\Pref file - Mac\com.contourdesign.shuttle.prefs to ~/Library/Preferences/.

After you have completed setup of the Shuttle Control, you must set the focus to the player (click once in the player area) before the Shuttle Control can be used.

In the next chapter you will find troubleshooting and disaster recovery procedures.

Troubleshooting and Disaster Recovery

This chapter includes information for preliminary system troubleshooting and disaster recovery. You should perform these activities before contacting Oracle Support for assistance. The following information is included:

- [Task Manager and DIVAdirector API Windows Services](#)
- [Starting and Stopping the DIVAdirector Web Server](#)
- [Checking Log Files](#)
- [Manual Backup and Database Restore](#)

Task Manager and DIVAdirector API Windows Services

The DIVAdirector installer will install two additional Windows services and the DIVAdirector web application. You can configure both of these services in the Windows Services console or using the command line with the options listed as follows:

```
servicename.exe {option}
```

Note: The `servicename.exe` in the previous syntax represents the name of the service you are working on.

install

This option installs the service.

uninstall

This option uninstalls the service.

start

This option starts the service if it is not already running.

stop

This option stops the running service.

Task Manager Service

The Task Manager service is responsible for handling any long running background tasks needed by DIVAdirector. The binaries for this service are installed in the `TaskManager` subdirectory, located under the DIVAdirector installation directory (for example, `C:\Program Files (x86)\DIVAdirector 5\TaskManager`). This service is

visible in the Windows Services console under the name `Oracle.DIVAdirector.TaskManager`.

DIVAdirector API Service

The DIVAdirector API service is a web service responsible for handling authentication, authorization, and file upload requests for the *Local Archive* process. *This service currently only handles a subset of the application's responsibilities.*

The binaries for this service are installed in the `Api` subdirectory located under the DIVAdirector installation directory (for example, `C:\Program Files (x86)\DIVAdirector 5\Api`). This service is visible in the Windows Services console under the name `Oracle.DIVAdirector.Api`.

Starting and Stopping the DIVAdirector Web Server

You can start and stop the DIVAdirector Web Server manually if issues arise pertaining to the web-based user interface using the following procedure:

1. Open the Internet Services Manager (`inetmgr`).
2. Click the computer's computer name and then locate **DIVAdirector 5** under the **Sites** menu.
3. In the *Actions* panel (on the right side of the screen), under the *Manage Web Site* section, click **Start** to start the web server, **Restart** to stop a running server and then start the web server again, or **Stop** to stop it completely.

A menu item that is grayed out and not selectable indicates the current state of the web server. For example, if the **Start** menu item is grayed out, the web server is currently running.

Checking Log Files

DIVAdirector creates log files for both the system and for Drop Folders during normal operations. You configured the log file names, sizes and locations in the initial DIVAdirector configuration. See [Logging Configuration](#) if you need a reminder of the file names and locations you assigned to the logs.

The DIVAdirector server logs contain information regarding the various server operations and possible operation processing error information. The Drop Folder logs contain information specific to the Drop Folders.

You can find the web server logs in the `DIVAdirector_HOME\www\logs\log.txt` file. The web server logs are used for troubleshooting the system and may be requested by Oracle Support when you request assistance.

You may need to change the levels you set during initial system configuration to assist in troubleshooting activities. During troubleshooting it may be necessary to raise the logging level higher to assist in locating the source of an error or fault. The recommended log file level settings for normal system operation are as follows:

- For DIVAdirector server logs set the log level no higher than *Level 2* unless you are trying to locate an error or instructed to do so by Oracle Support.
- For Drop Folder logs set the log level no higher than *Level 0* unless you are trying to locate an error or instructed to do so by Oracle Support.

Manual Backup and Database Restore

The manual backup and restore of the database are very important operations in any data system. DIVAdirector provides you a simple way to perform these operations when necessary.

Performing a Manual Backup

Use the following procedure to perform a manual backup of the DIVAdirector database:

1. Navigate to the **Admin, Backup, Manual Backup and Restore** screen.
2. Click the option for *Backup* on the **Manual Backup and Restore** screen next to *Operation*.
3. Browse the directory and select the backup destination folder.

Note: The backup file name `DIVAdirector_database_timestamp.sql` is predefined and cannot be modified.

The time stamp format is `DDMMYY-hhmm`, where:

- DD = day of month
 - MM = month
 - YY = year
 - hh = hour
 - mm = minute
4. Click **Backup Now** on the top right side of the screen to begin the backup operation.

A message will appear at the bottom of the screen stating that the backup process has started and normally takes approximately 3-5 minutes to complete (depending on the amount of data in the database). The message is displayed in red text at the bottom of the **Manual Backup and Restore** screen.

Performing a Database Restore

Caution: A manual backup of the database should be completed first before performing a database restore operation.

Use the following procedure to manually restore the DIVAdirector database:

1. Click the option for *Restore* on the **Manual Backup and Restore** screen next to *Operation*.
2. Browse the *From* area to display the server's remote file system tree.
3. Select the database snapshot file to be restored (click once on the file name).
4. Browse the *To* area and select a restore destination folder, or select **Restore to Active Database (logs off all connected users)**.

If you select the **Restore to Active Database (logs off all connected users)** option, the restore process will replace the existing database with the restored database. A

confirmation dialog box is displayed notifying you that all connected users will be logged off.

5. If you have not selected the **Restore to Active Database (logs off all connected users)** option, click **Restore Now** to begin the restore process.

Frequently Asked Questions

This chapter contains frequently asked questions.

Do Proxy Drop Folders exist and are they still usable?

Yes they still exist in this release and can be used. However, Oracle recommends using the new Transcode Service rather than Proxy Drop Folders.

Does the original proxy workflow still exist and is it still usable?

Yes the original proxy workflow still exists and is usable in this release.

What releases of DIVArchive does DIVAdirector support?

DIVAdirector 5.4 supports DIVArchive 7.4 and later.

Can DIVAdirector 5.4 list all component files of a DIVArchive Complex Object?

Currently DIVAdirector can list all complex object component files.

Can DIVAdirector 5.4 restore any component file of a DIVArchive Complex Object?

Complex object support is currently implemented in 5.4.1.

If proxies are created outside of the new transcode service, do local proxies still work the same way?

It is highly discouraged to use proxies produced outside of DIVArchive and DIVAdirector. However, the Local Proxies feature still works in this release.

Do Drop Folders support Oracle DIVArchive Partial File Restore?

DIVArchive Operation Drop Folders support Partial File Restore operations.

Which file is the proxy generated from when referring to the ProxyFileExtensions parameter?

The transcoder will proxy a file with valid file extensions when a request is made to the Transcoder Source/Destination from DIVAdirector. The user selects the file in question in that case and automated proxy generation currently remains unchanged.

Exactly what transcoders are supported by the Transcode Service?

Vantage and Flip Factory are both supported through their API interfaces. Additional transcoders are supported (such as FFMpeg) given that their command line interfaces will provide DIVAdirector with the frames and metadata required. These command line interfaces are generally accessed through custom scripts, but they can be interfaced with directly as well if the parameters are supplied correctly.

Glossary

Complex Object

A complex object contains 1,000 or more files. This value is configurable in DIVArchive. Complex object handling may be different than non-complex objects. See [Object](#).

Data Store

A data repository of a set of integrated objects.

Drop Folders

Network monitored folders that have specific operations assigned to them. When files are placed into a Drop Folder, the system will perform the operations identified for that specific folder.

Internet Information Service (IIS)

The Internet Information Service is an extensible web server created by Microsoft for use with the Windows NT family of operating systems. IIS supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP protocols. IIS is not turned on by default when Windows is installed. The IIS Manager is accessed through the Microsoft Management Console or Administrative Tools in the Control Panel.

LDAP (Lightweight Directory Access Protocol)

The Lightweight Directory Access Protocol is an application protocol for accessing and maintaining Distributed Directory Information Services over an IP network.

Object

Objects are archive entries. An object (archive entry) is identified by a pair (Name and Category) and contains video files, audio files, metadata files, and so on. The files are stored in DIVArchive as *Object Instances*. An object can contain up to 1,000 files before being considered a complex object. See [Complex Object](#).

Partial File Restore (PFR)

Restore only part of a file (rather than the entire file) from DIVArchive to a destination based on timecode, byte offsets, folders, or DPX frames.

Proxy

A Proxy Video is a form of metadata. It consists of highly compressed, very low resolution video and sound, that mirrors a high resolution original master digital recording.

Shot List

A list compiled by a user containing video clips (shots) which indicates the sequence of scenes included in the list. The list may include the scene number, the location of where the scene was shot, a description of the scene, the length of a scene, a list of actors in the scene, and so on.

UNC (Universal Naming Convention)

The Universal Naming Convention specifies a common syntax to describe the location of a network resource such as a shared file, directory, or printer. The UNC syntax for Windows systems has the generic form `\\ComputerName\SharedFolder\Resource`.

Work Bin

A working area for users allowing them to organize and work with video clips, files, objects, and so on, in a single location.