Telestream

DIVA Core

DIVA View

Administrator Guide

Release: 6.1.0.209

Revision: 1.1

Copyrights and Trademark Notices

telestream

Contents

telestream

telestream

telestream

Daily Operations   123

System Management   130

Troubleshooting and Disaster Recovery   137

telestream

Frequently Asked Questions   143

Additional Configuration Information   145

Glossary   161

Telestream Contact Information

To obtain product information, technical support, or provide comments on this guide, contact us using our web site, email, or phone number as listed below.

Resource	Contact Information
DIVA Core Technical Support	Web Site: https://www.telestream.net/telestream-support/diva/support.htm Depending on the problem severity, we will respond to your request within 24 business hours. For P1, we will respond within 1 hour. Please see the Maintenance & Support Guide for these definitions. • Support hours for customers are Monday - Friday, 7am - 6pm local time. • P1 issues for customers are 24/7.
Telestream, LLC	Web Site: www.telestream.net Sales and Marketing Email: info@telestream.net Telestream, LLC 848 Gold Flat Road, Suite 1 Nevada City, CA USA 95959
International Distributor Support	Web Site: www.telestream.net See the Telestream Web site for your regional authorized Telestream distributor.
Telestream Technical Writers	Email: techwriter@telestream.net Share comments about this or other Telestream documents.

telestream

Preface

This document gives a basic understanding of system functionality and detailed instructions for installing and configuring DIVA View 6.1.0.209.

Audience

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

Documentation Accessibility

For information about Telestream's commitment to accessibility, visit the Technical Support Portal located at:

https://www.telestream.net/telestream-support/diva/support.htm

Access to Telestream Support

Customers that have purchased support have access to electronic support through the Technical Support Portal located at:

https://www.telestream.net/telestream-support/diva/support.htm

Related Documents

For more information, see the DIVA View documentation set for this release located at:

https://www.telestream.net/telestream-support/diva/support.htm

Document Updates

The following table identifies updates made to this document.

Date	Update
March 2022	Replaced incorrect screenshot
May 2022	Updated Copyright information. Updated step 6 in Adding Collection Filters to include more specific instructions.
June 2022	Added support for Windows 2022 Server. Rolled back terminology from Content App to DIVA View.
August 2022	Updated terminology to new standards (see the *Overview* for new terms). Migrated book to Telestream format and styles.
September 2022	Updated software date formats.
November 2022	Reverted the term "Virtual Object" to "Object" as necessary.
December 2022	Updated release number to 6.1.0.209.
January 2023	Removed section on database restore. Updated copyright dates.

Overview

DIVA View is a Graphical User Interface for Core 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 DIVA View 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 DIVA View you can:

- Search for video clips by file name, date, Collection, 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.

Topics:

- New Terminology
- Supported Proxy and Audio Formats

telestream

New Terminology

The following terminology has been updated to reflect standardization efforts across all DIVA and Kumulate applications. There will be some variations in the documentation compared to the interface until everything is switched over to the new terminology; the documentation uses the new terms wherever possible.

- Running Requests are now called Jobs
- Request History is now called Job History
- Libraries are now called Managed Storage
- Datahub is now called Actor
- Proxyhub is now called Proxy Actor
- DIVA Core and DIVA Manager are now called DIVA Core / Core / Core Manager
- Category is now called Collection
- Source/Destination is now called Unmanaged Storage Repository
- Storage Repository is now called Managed Storage Repository
- Group is now called Tape Group
- Link is now called Storage Link
- Storage Plan Manager is now called Storage Policy Manager
- Drop Folder Monitor (DFM) is now called Watch Folder Monitor (WFM)
- DIVA Command and Control Panel are now called System Management App
- DIVA Analytics and DIVAProtect are now called Analytics App

telestream

Supported Proxy and Audio Formats

Recent browser releases (in general) no longer support NPAPI. Applications such as Silverlight and QuickTime cannot be used with these browsers. This is a browser limitation, not a DIVA View limitation. Telestream recommends using MP4 as the standard video format.

DIVA View 6.0 and later supports the following proxy and audio formats. DIVA View 6.0 does not currently support discontinuous timecodes.

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

- 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. Telestream 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 (constant)
  – The optimum bitrate will depend on available bandwidth and other video settings (frame rate, resolution, and so on). Variable Bitrates are not supported.
  – Audio Codecs: AAC, WAV
  – 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
  – WMVs can have paired standalone WMAs for multiple audio tracks.
  – Video Bitrates: 100 to 1042 Kbps, constant
  – Audio Codecs: WMA
  – Audio Bitrates: 32 Kbps, 48 Kbps, 512 Kbps, constant
  – Audio Sampling Rates: 22kHz, 44kHz (44kHz is standard)

telestream

- QuickTime
    - Container: MOV
    - Video Codecs: AVC
    - Video Bitrates: 506 to 1042 Kbps (constant)
    - Audio Codecs: AAC
    - Audio Bitrates: 64 Kbps, 128 Kbps (constant)
    - Variable Bitrates are not supported.
    - Audio Sampling Rates: 22 kHz, 44 kHz (44 kHz is standard)

Installation

This chapter describes initial installation of DIVA View 6.1.0.209.

Topics:

- Preparing for Installation
- Prerequisites
- Planning System Deployment
- Minimum System Configuration
- New System Installation
- Upgrading DIVA View
- Uninstalling DIVA View 6.1.0.209

telestream

Preparing for Installation

Before the test Delivery and Installation Team arrives at your site, or accesses the target servers, you must complete installation and configuration of your system hardware. You must assign IP addresses and storage locations, open ports in the firewall, complete network cabling, and so on. When the team arrives they will review the configuration specifications before starting the installation to ensure all necessary components are in place and accessible. Installed hardware must meet or exceed the list of recommended minimum hardware specifications provided to you.

Notes: Windows 2022 Server is now supported.

See the DIVA Core Supported Environments documentation for hardware and software requirements.

Configure the server host computer for operation within your network and restrict access to the server with a unique, secure password. Install Microsoft IIS (Internet Information Server) computer, and confirm operation and network connectivity.

You can find Microsoft IIS installation instructions in the following locations:

Note: If upgrading from Windows Server 2008R2 or lower, a new OS / Server will need to be provided.

- IIS 8 (Windows 2012 R2 Server)

  https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012

- Windows Server 2016

  https://docs.microsoft.com/en-us/dynamics-nav/how-to--install-and-configure-internet-information-services-for-microsoft-dynamics-nav-web-client

- Windows Server 2019

  https://docs.microsoft.com/en-us/iis/get-started/introduction-to-iis/introduction-to-iis-architecture

Any applications must be licensed and installed (for example, Vantage). You must configure all DIVA Core configuration parameters set up including IP addresses, port configurations for storage devices, video servers, Avid Interplay (if in use), Microsoft Cluster Manager (if in use), and so on. The team needs this information for reference during DIVA View installation.

You must have at least one fully operational client computer available for testing during and after installation. Client computers must have a valid, supported Microsoft OS version (either 32-bit or 64-bit), or Mac OS 10.6 (Snow Leopard) or later operating system installed, and one of the following web browsers (visit the Technical Support Portal to check for updated browsers and restrictions):

- Internet Explorer 11 or later

- A supported Google Chrome version
- A supported Microsoft Edge version
- A supported Firefox version

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

DIVA View does not currently support Safari.

Technical Support recommends keeping the operating system up to date with the latest security patches.

Prerequisites

The server can connect to DIVA Core 7.4, or later, through the DIVA Enterprise Connect software. You will install PostgreSQL database, DIVA View, and the following components:

- DIVA View Web Server 6.1.0.209
- DIVA View TaskManager
- DIVA View API
- PostgreSQL 9.6.x (up and until DV 6.0.1.4 version, PostgreSQL 12 for later DV versions)
- .NET Framework release 4.5.2
- Powershell 5.0

Caution: **Ensure that the computer name is set before running DIVA View installer. The computer name cannot be changed after DIVA View is installed because it invalidates the rights and permissions of the IIS user account.**

Ensure that the computer's drives and network connections are correctly configured. Storage locations must have appropriate access rights, and network devices must have log in credentials configured to connect automatically.

Ensure the computer's Administrator account has a secure password.

The upgrade is not compatible with DIVAdirector releases before release 5.2. or versions using the Linter Database Engine.

Earlier releases of DIVA View have additional steps required before they are eligible to upgrade with this installer. In this case, contact your Telestream Commercial representative.

telestream

Planning System Deployment

DIVA View consists of four main components installed on the same host and interacting with each other:

- DIVA View Web Server (IIS)
- DIVA View Database - PostgreSQL DB Engine running as a Windows service
- DIVA View TaskManager running as a Windows service
- DIVA View API running as a Windows service
- DIVA View Transcode Service - only required if using proxies or needing to extract Media metadata from source clips
- DIVA Enterprise Connect - required to connect to the DIVA Core Manager

Telestream highly recommends installing DIVA View on a host different from the DIVA Core system to improve the performance of both systems. They may be installed together on the same computer if it is a standalone system, but performance degradation may apply. The transcode service can be on the same server with FFMpeg for frame extraction, but it is recommended that transcoding itself is done on a remote server to not overload the web server.

Minimum System Configuration

The minimum system specifications for deploying DIVA View are listed in the DIVA Core Supported Environments Guide document.

Note: Windows 2022 Server is now supported.

New System Installation

The following sections describe a new installation using either the UI (User Interface) Installer or the Command Line Installer.

Note: You must have a valid license to install DIVA View. The license file is named DIVAView.licx and can be obtained through Telestream Sales. The license is required for the installer to run, so it must be acquired before starting the installation.

Using the UI Installer

Use the following procedure to install DIVA View 6.1.0.209 on a new system using the UI Installer:

Note: DIVA Enterprise Connect settings must be provided during the DIVA View installation process. Telestream recommends installing and configuring DIVA Enterprise Connect before beginning the DIVA View installation.

---

1. Confirm that the Windows Update Service and Remote Registry Service are enabled before installation. You can disable them after the installation completes. These services are required to allow a component within the installer called the Windows Desktop Experience to be installed.

   It is also necessary that IIS, Powershell 5.0 and the .Net Framework are installed prior to running the installer. Powershell 5 and the Framework are automatically installed with Windows 2016 and 2019, but must be downloaded and installed manually for 2012 installations. IIS will always have to be enabled through Windows Features. The installer will check for the rest of the required components automatically and will enable any features not currently enabled.

2. The installer first checks if any prerequisites need to be installed. If one of the prerequisites is not found, it will install the appropriate application. This may require a restart of the computer to continue the installation.

3. Double-click the DIVA View installer to begin installation. The Welcome screen appears.
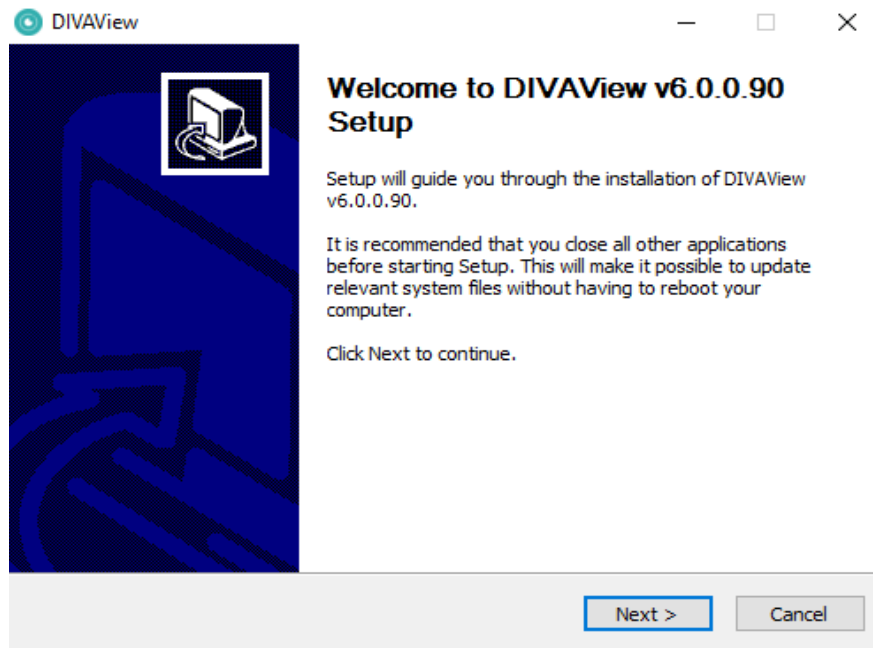
4. Click Next to continue.

5. A notification dialog box is displayed if a previous version of DIVA View is installed.

Click Yes to uninstall the previous version, or click No to leave the previous version in place.

Note: Direct upgrades are automatically detected, but this is limited to 6.1.x releases. For earlier installations Telestream recommends exporting and importing the database, and performing a full uninstallation before proceeding.

---

6. Enter the installation location in the Destination Folder text box. Alternatively use the Browse button to open a Windows Explorer dialog, navigate to the desired folder (or create a new folder), select the folder to install DIVA View and select OK. When you have entered the installation directory click Next to proceed.

Notes: Telestream recommends installing DIVA View in the default folder (C:\Program Files (x86)\Telestream\DIVAView\www\DIVAView.licx).

For new installations (not upgrades), the Telestream\DIVAView\www path does not exist. The person performing the installation must create the www folder and copy the license file into the folder. The license file must be named DIVAView.licx.

---
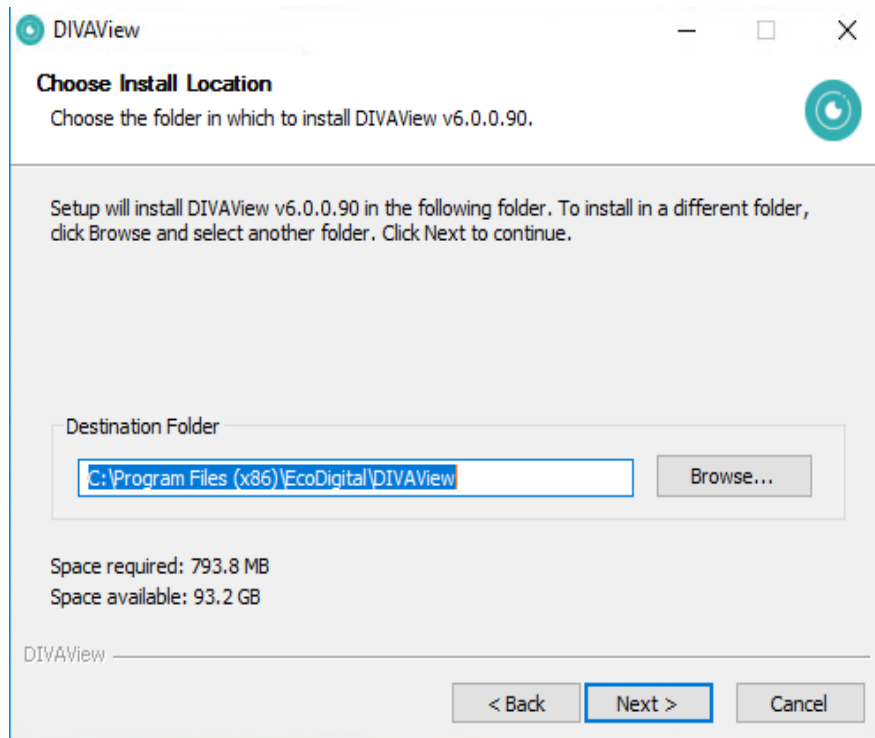
7. Enter the location of the DIVA View license file. Alternatively use the Browse button to open a Windows Explorer dialog, navigate to the desired folder, select the license file and select OK. When you have entered the location of the license file click Next to proceed.

Notes: Telestream recommends installing DIVA View in the default folder (C:\Program Files (x86)\Telestream\DIVAView\www\DIVAView.licx).

For new installations (not upgrades), the Telestream\DIVAView\www path does not exist. The person performing the installation must create the www folder and copy the license file into the folder. The license file must be named DIVAView.licx.
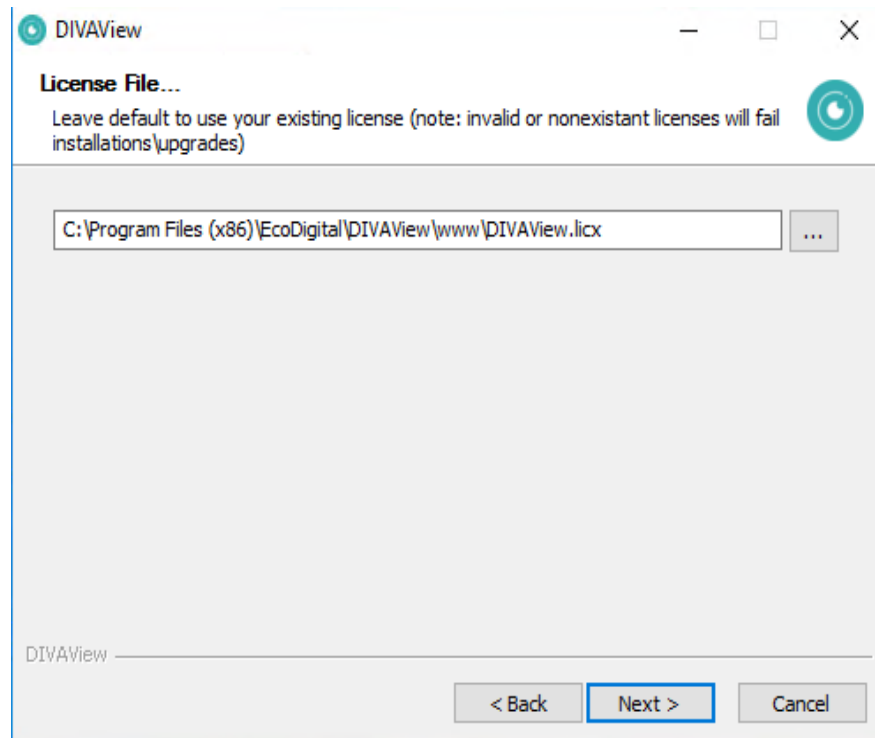
8. On the Storage Configuration screen enter the correct full paths for Proxies, Database Backup, Local Archive, Local Restore, and QC Reports in the corresponding text boxes. When complete click Next to proceed.

Notes: In DIVA Core, the LOCAL_RESTORE and LOCAL_ARCHIVE folders must be named the same, and point to the same destination folders, as the folders defined during DIVA View configuration.

The H partition is the default, but the idea is to have the Proxies stored on a dedicated partition or NAS because over time this is the partition that gets filled the most.

While a NAS is the best option for proxy storage, there are some NAS types that are not compatible with IIS. You should check with the NAS vendor to determine compatibility.

The Database Backup must be located on a separate disk from the running Database to prevent from double data loss in case the HDD has an issue.
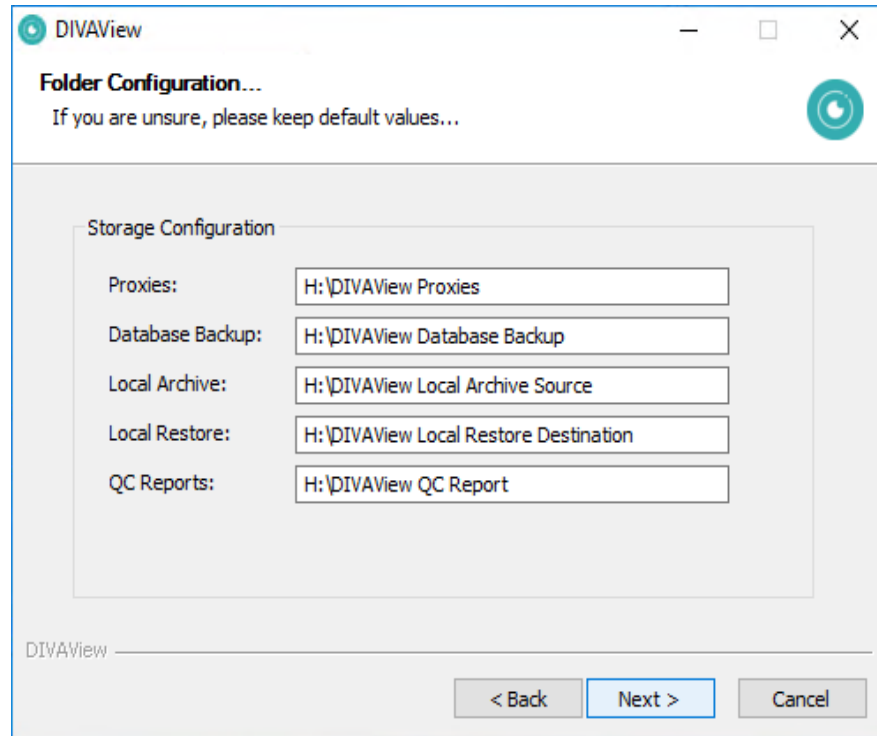
Caution: In the next steps, do not specify a path pointing to a network mapped
drive if you intend to use a network share. Only UNC (Universal Naming
Convention) paths can be specified for the proxy folder. The reason is
that drive mapping is performed for the interactive user session only.
This drive mapping does not exist in the DIVA View Web Server service
session. Although this dialog accepts a network proxy path, the
corresponding changes must be performed to the DIVA View Web
Server service user account manually.

---

9. On the Database Configuration screen specify the full paths for PG Binary Directory
(path to the Postgres Binaries), PG data Directory (path to the Postgres Data), DB
Import Path (path to the database backup being imported if needed), and DB
Import Version (the four number version of the database being imported in the
format xx.xx.xx.xx if needed) in the corresponding text boxes. When complete click
Next to proceed.

Notes: Telestream recommends leaving these preconfigured Postgres directory
locations at the default entry.

The Database Backup must be located on a separate disk from the running
Database to prevent from double data loss in case the HDD has an issue.

---

telestream
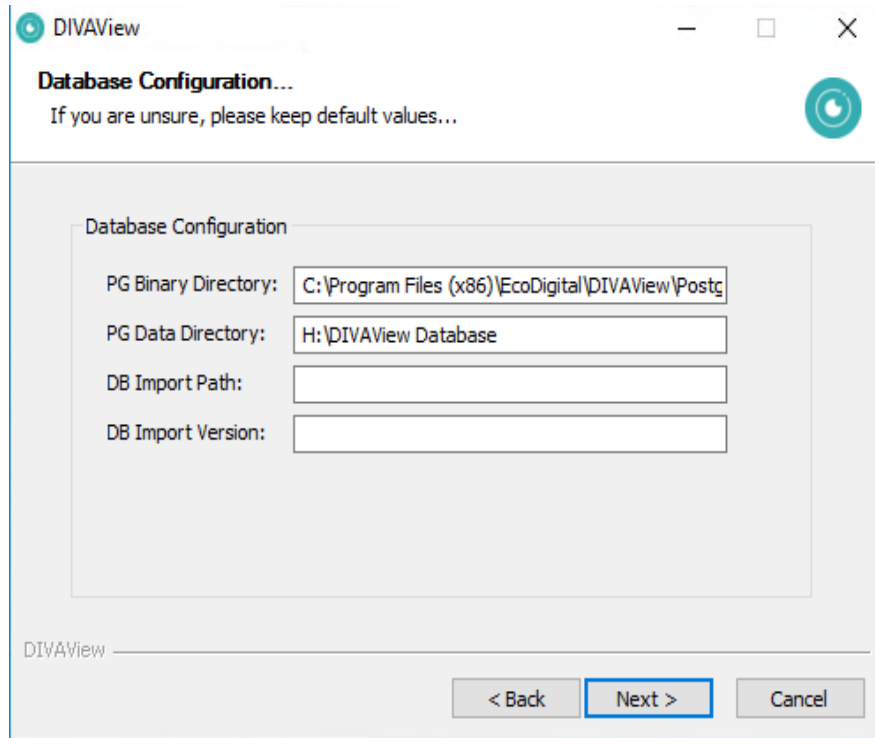
10. On the DIVA Core Configuration screen enter the Enterprise Connect Endpoint configuration including IP Address, Port, Client ID, and Api Key in the corresponding text boxes. Select the Use legacy DIVAS check box if there are legacy DIVA systems in your configuration. When complete click Next to proceed.
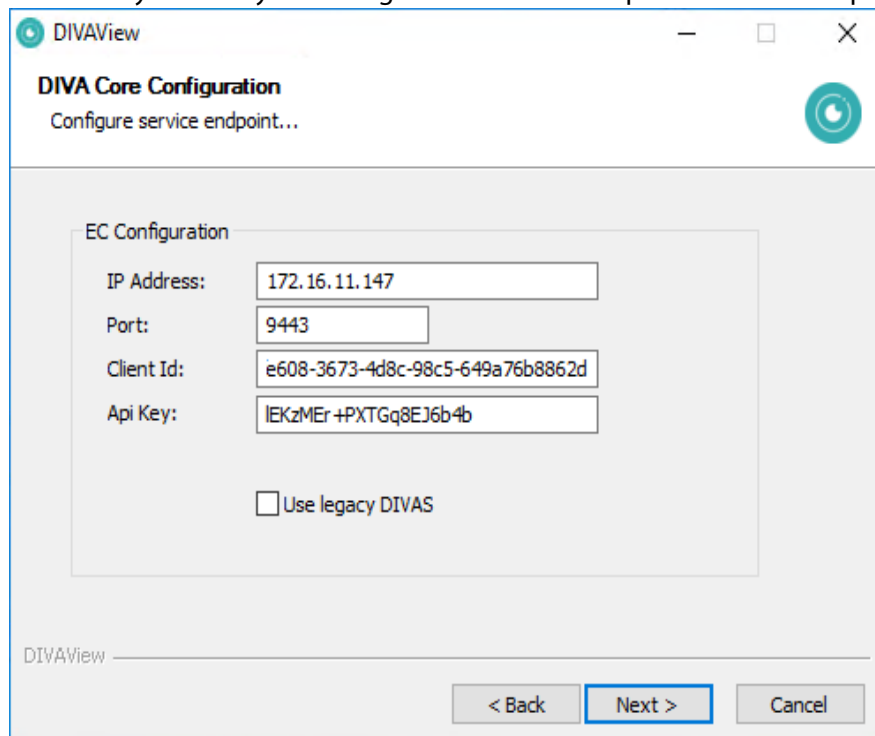
11. On the DIVA View Api Configuration screen specify the DIVA View IP Address, Host
Name, and Port. If a custom certificate is provided then you should match the
hostname to the certificate so it can easily be registered upon installation. When
complete click Next to proceed.

12. Telestream recommends that services run under a domain account that has access
to all the shares required for proxy storage and transcoding. You enter these
credentials on the Service Account Configuration screen by specifying the User
Name (typically dd6-user) and Password in the respective text boxes for a local user
account that will run the DIVA View Web application. When complete click Next to
proceed.

Note: A complex password is necessary. If you are using either a SAN, or NAS, for
proxy storage, then it is better to run IIS as a domain account.
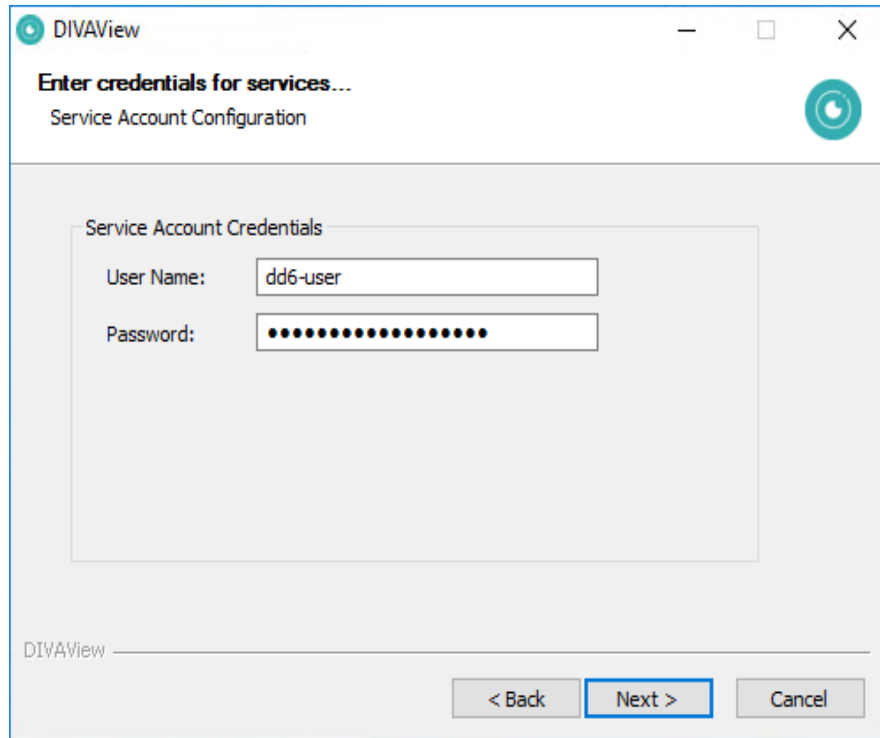
13. Click Install to continue.

14. Select the check box to install the Transcode Service after DIVA View installation is complete; otherwise leave it deselected. When complete click Install to proceed.

Notes: The Transcode Service installs the Transcode Host Windows service or client depending on the choice selected if it is on a host machine.

The standalone installation (or upgrade) of a Transcode Service can be performed by running the Transcode Service installation binary directly. If you do not have this binary, please contact Telestream Support.

---
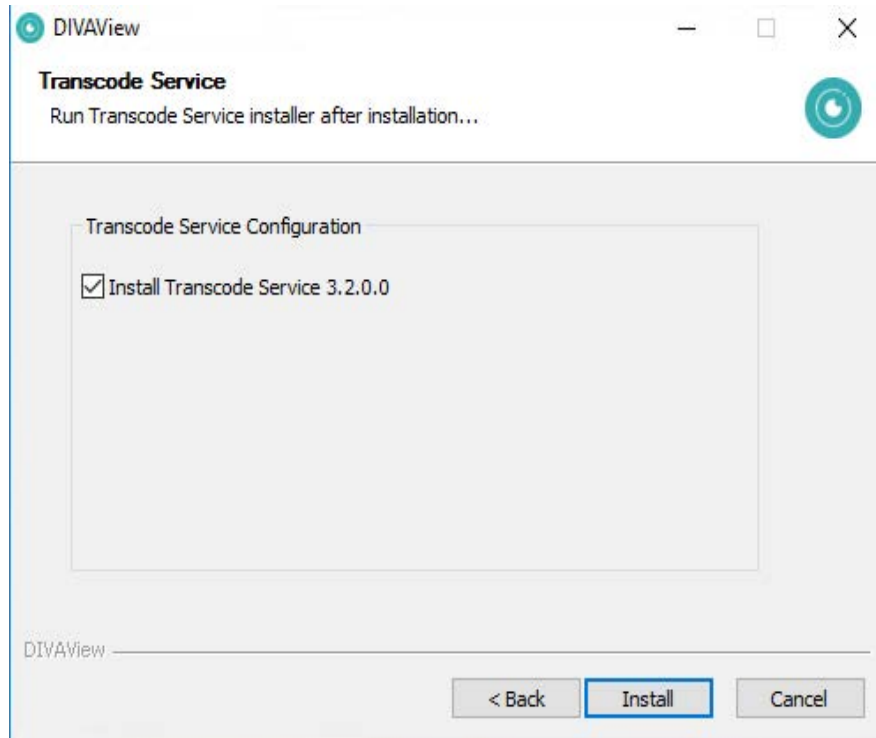
15. The software will run through the installation process and display the progress during the installation.

telestream
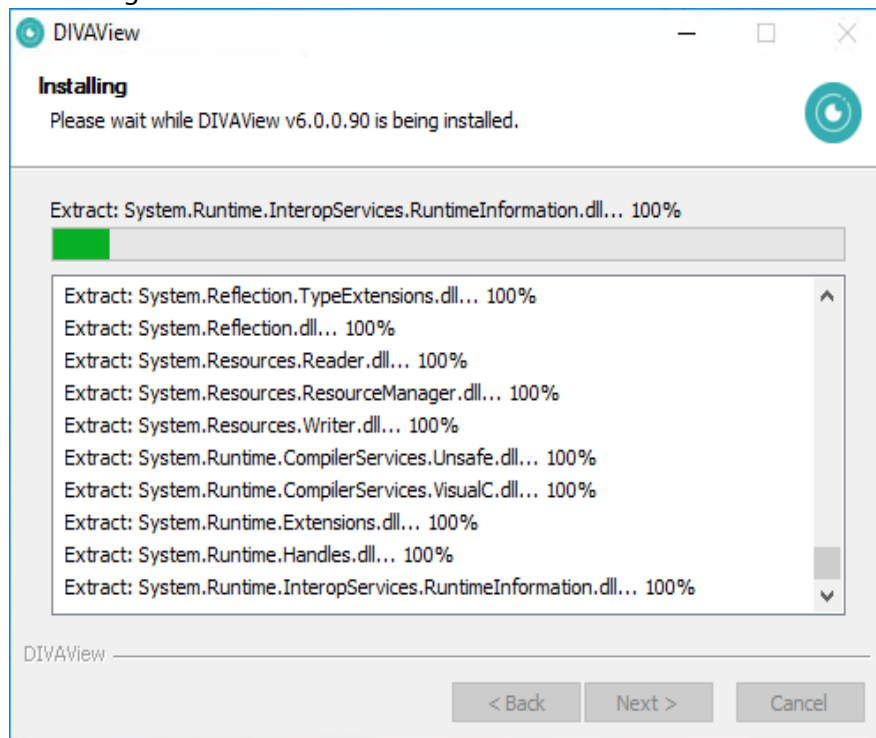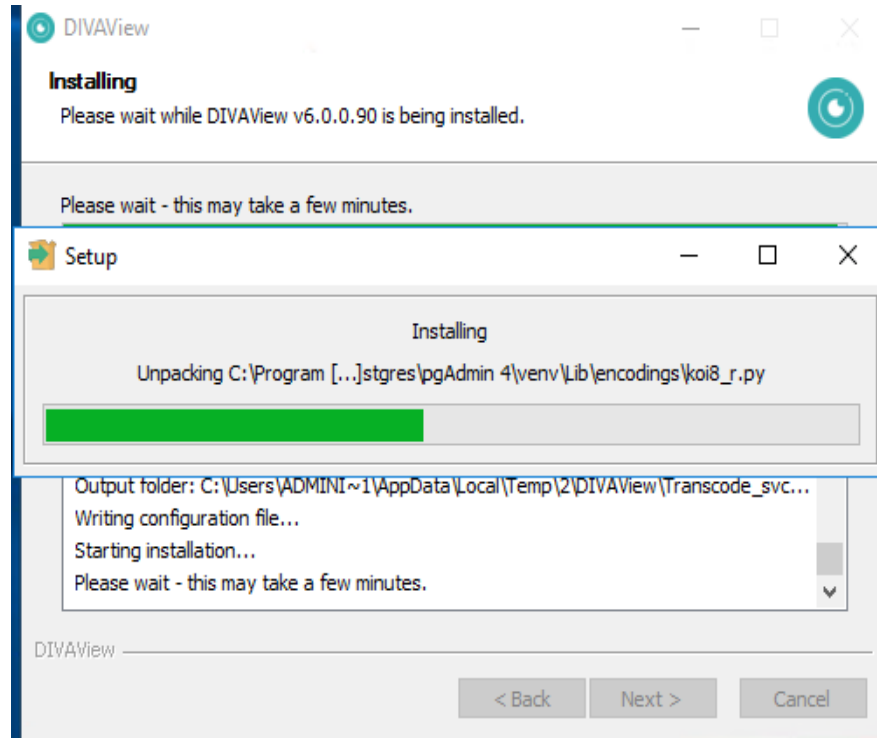
16. After installation is complete locate the Internet Information Services Manager using the Windows Start menu.
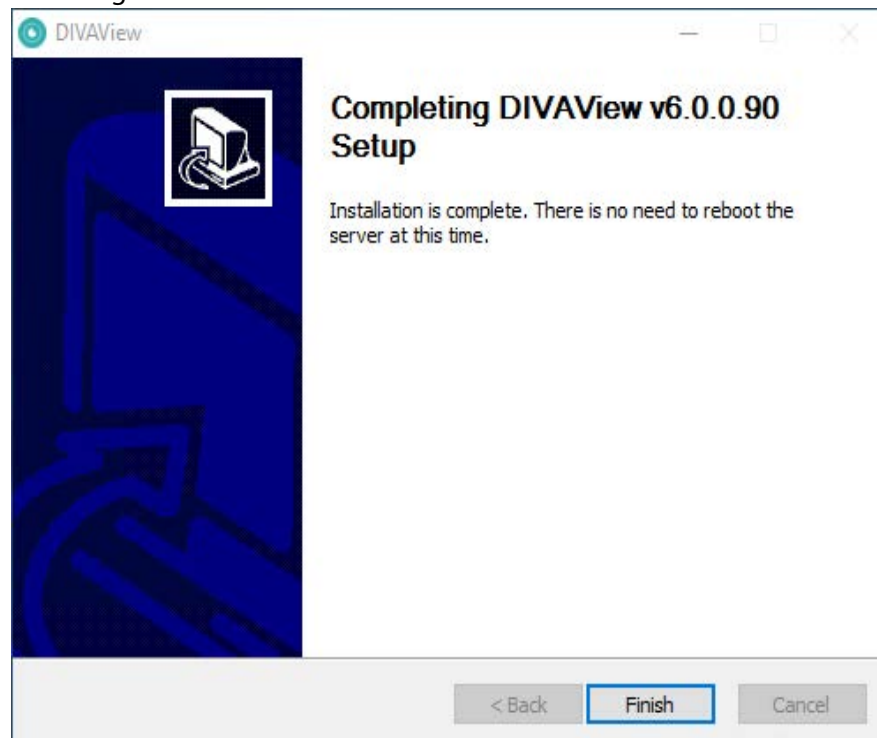
17. After the IIS Manager loads, click the computer name of the computer where you are installing DIVA View, click Sites > DIVA View 6.

18. Verify that the DIVA View 6 website is running by confirming that the Start button on the right side of the screen is disabled (grayed out), indicating that the site is operational.

Using the Command Line Installer
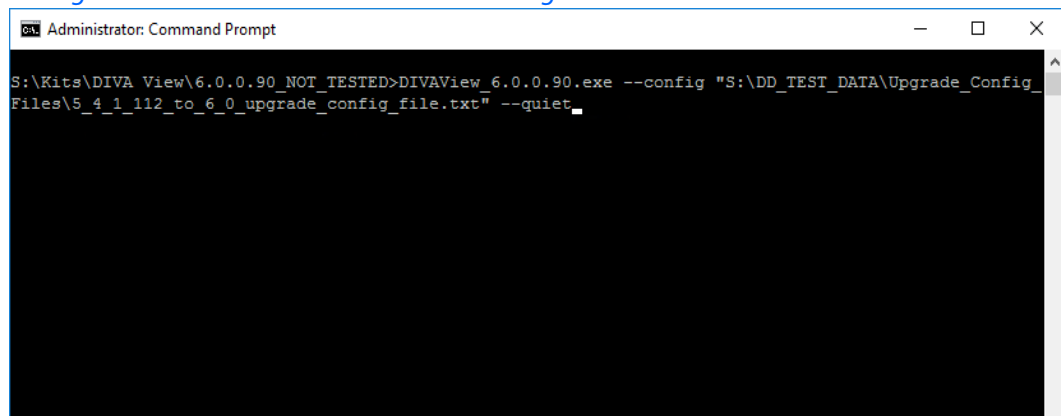
This is the preferred method of installation and has the benefit of having a record of the parameters that were provided. Use the following procedure to install DIVA View 6.1.0.209 on a new system using the Command Line Installer:

Execute the following to run the DIVA View Command Line installer:

```
DIVAView_<a.b.c.d>.exe -config <path to configuration file> --quiet
```

where <a.b.c.d> corresponds to the DIVAView release number, --quiet instructs the installer to run in quiet mode, and -config identifies the configuration file to use located in <path to configuration file>.

The following figure is a screen capture of what the command line would look like specifying the configuration file and running in quiet mode. There is a sample *Default Configuration File* located in *Additional Configuration Information*.

Upgrading DIVA View

Caution: Refer to *Proxy Storage Structure Changes During Upgrades* for important information on storage structure changes with DIVA View 6.1.x before performing any upgrade.

Upgrading DIVAdirector 5 to DIVA View 6.1.0.209

If you are upgrading an existing DIVA View system, it must be running one of the operating systems specified in *Prerequisites*. See *Proxy Storage Structure Changes During Upgrades* for details on storage structure changes during upgrades.

The storage migration is done in 2 steps. First is the migration of Shotlist frames, queries, asset images, and binary files. This step is performed automatically and will prevent login if there are any errors in the process; for example the storage locations being incorrect (most commonly). This step should be quite fast, so if an administrator sees the storage migration message when attempting the first login, it likely did not complete successfully and the logs in the Task Manager should be consulted to determine what the issue was that occurred.

The second storage migration step is initiated by the System Administrator on the Storage Location page after login. This must be done to migrate proxy frames out of the database and reorganize proxies in the Proxy Storage location directory for playback.

Refer to *Proxy Storage Structure Changes During Upgrades* for detailed information.

Notes: DIVA View upgrades require the purchase of Telestream Professional Services.

Telestream recommends upgrading a second server other than the Production Server to avoid prolonged down time in the production environment.

Upgrading using the User Interface

Direct database modification for the new location is required if moving to a new server that has different paths to the proxy storage. The initial storage migration steps require this path to be accessible. Use the following procedure to upgrade from DIVAdirector 5.2 (and later) to DIVA View 6.1.0.209:

1. Perform a full database backup to a known location before starting any upgrade process.
2. Run the installer and click Next to continue.
3. The installer first checks if any prerequisites need to be installed. If one of the prerequisites is not found, it will install the appropriate application. This may require a restart of the computer to continue the installation.

4. A notification dialog box is displayed if a previous version of DIVA View is installed.

   Click Yes to uninstall the previous version, or click No to leave the previous version in place. Click Next to continue.

5. From this point forward, follow the same procedure as installing DIVA View onto a new system (see *New System Installation*).

Upgrading using the Command Line Installer

Use the same process previously described in *Using the Command Line Installer* to upgrade your installation to DIVA View 6 through the command line installer.

The following is an example Use Case of conducting an upgrade using the Command Line Installer where Server A is running DIVAdirector 5.2, 5.3 or 5.4, and you want to prepare Server B to take over with DIVA View 6.1.0.209:

1. Export the DIVA Director Database from Server A.

2. Install DIVA View 6 on Server B using the Command Line Installer and a configuration file. You specify the exported Server A database in the configuration file.

3. Install DIVA View 6 on Server B, running all database upgrade scripts against the Source Server database exported from Server A.

4. When the process is complete, Server B is running with the upgraded data from Server A.

Notes: Upgrading from DIVAdirector 5.2 or 5.3 to DIVA View 6.1.0.209 changes the Proxy Storage directory structure. In this case, Technical Support recommends having a distinct copy of the Proxy Storage on Server B.

After the upgrade, any previous DIVAdirector 5.2 installations will not be able to access proxies located in Shared Proxy Storage due to the directory structure change.

---

telestream

Uninstalling DIVA View 6.1.0.209

Adhere to the following instructions to uninstall DIVA View 6.1.0.209:

- Never run uninstall.exe directly from the DIVA View installation directory.

- Always use Windows Control Panel, All Control Panel Items, Programs and Features dialog to trigger DIVA View 6.1.0.209 uninstallation.

- When complete, manually delete the C:\Users\Administrator\AppData\Local\Temp\DIVAView folder if it exists.

- Manually delete the C:\Users\Administrator\AppData\Local\Temp\n folder if it exists (where n is the number of the folder created).

When uninstalling DIVA View, the DB Backup and Proxy Storage directories are not automatically removed. These directories contain last chance value added production data.

After confirming you have retrieved all of your data from these directories, they must be manually deleted by the System Administrator.

telestream

Initial Configuration

DIVA View configuration must continue after the initial installation is complete. The initial configuration tasks in this chapter are typically completed one time unless there are major system or network changes (for example if IP addressing changes, port numbers change, and so on).

Note: Transcoder Configuration for proxies generation and metadata extraction is detailed in *Proxy and Transcoder Configuration*.

This chapter describes initial configuration after installation.

Topics:

- Changing the Administrative Password
- Confirm DIVA Enterprise Connect Connectivity
- Configuring DIVA View User Interface
- System Maintenance Settings
- DIVA Core Synchronization
- Automated Backup Configuration
- Configuring DIVA View Web Server
- Account Configuration and Management
- Administrator's Message
- Metadata Configuration
- Quality Control (QC) Report Configuration

telestream

Changing the Administrative Password

DIVA View is installed 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 DIVA View administrative password when you log in for the first time.

Notes: There are rules for all passwords as follows:

All passwords have a 3 month forced expiration. This cannot be modified for security purposes.

Must be between 8 and 128 characters

Must contain a letter

Must contain a number

Must contain a symbol

Must not contain whitespace characters

New password must not be a previously used password.

Confirm DIVA Enterprise Connect Connectivity

DIVA View interacts with DIVA Core using a standards-based Web Service API. The integration with this service, DIVAEC (DIVA Enterprise Connect), is configured in two different configuration files in DIVA View. Both of these files should be configured automatically during the installation process. However, Technical Support 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)\DIVAView 6\www\web.config).

The second file Telestream.DIVAView.TaskManager.exe.config is located in the TaskManager subdirectory in the installation directory (C:\Program Files (x86)\DIVAView 6\TaskManager\Telestream.DIVAView.TaskManager.exe.config).

The following keys are duplicated and must be updated in the appSettings section of both files:

- DIVACoreApiUrl

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

   ```
   <add key="DIVACoreApiUrl" value="https://server_ip:9444/diva/
   service/rest/2.2/DIVACoreWS_REST" />
   ```

telestream

Note: The server_ip address in the previous example must match the IP address where DIVAEC was installed.

- DWSVersion

  ```
  <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" />
  ```

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

1. Open a Web Browser from the DIVA View Server.

2. Navigate to http://server_ip:7001/ws_utc/login.do.

3. If you are able to log in to the Web Services Test Client interface, then the service is operational. Otherwise, consult the DIVA Enterprise Connect documentation to resolve any issues with the service.

telestream

Configuring DIVA View 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 DIVA View and DIVA Core. To configure the DIVA View user interface navigate to the Administration > System Management menu at the top of the screen.

First you will configure the System Settings.

System Settings

The System Settings screen enables configuration of system-wide 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 Administration > System Management > System Settings menu.
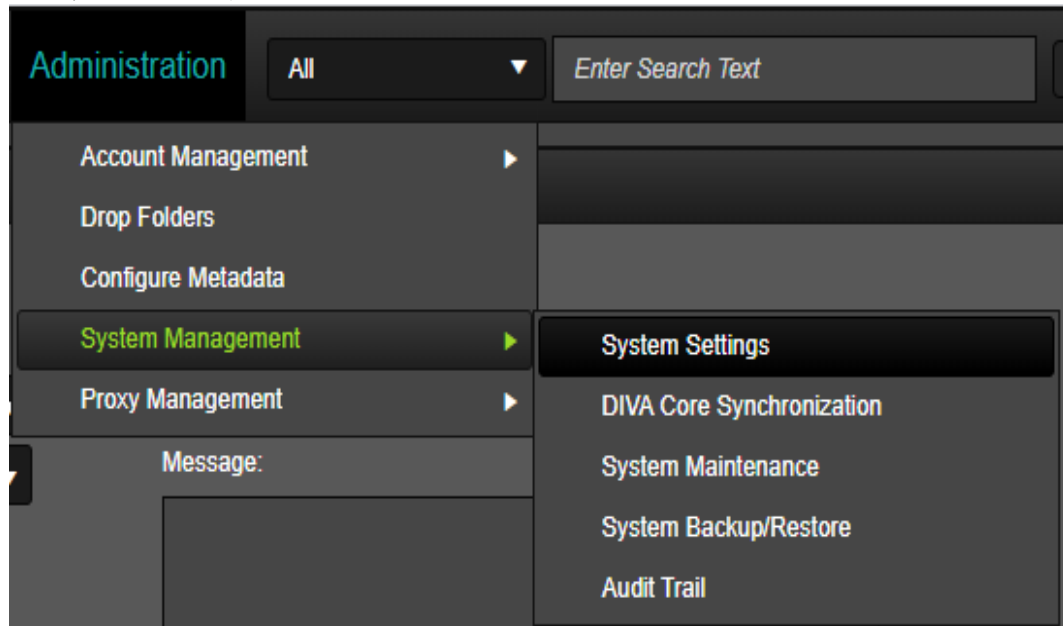
2. Enter the appropriate values that are optimal for your organization and users for each option.

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.

System Settings

The following fields are configurable in the Default Settings area of the screen; changes are applied after clicking Save on the top right of the window:

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 Technical 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. Only System Metadata can be used for sorting.

• Date Display Format

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

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

telestream

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.

DIVA Core Settings

The following fields are configurable in DIVA Core Settings area of the screen:

Note: The LOCAL ARCHIVE and LOCAL RESTORE directories have reserved names and must be configured in DIVA Core System Management App using the associated reserved names (that is, LOCAL_ARCHIVE and LOCAL_RESTORE).

- 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.

Note: Technical Support recommends using archiving tools such as FTP Server, SFTP Server, cloud-based file transfer and file management tools for Local Archives that include files greater than 2 GB.

- 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.

Connections

The following fields are configurable in the Connections area of the screen:

- Maximum Number of Concurrent Users Allowed

  DIVA View 6.0 and later is licensed for concurrent usage, but may be further limited by concurrent users here to address performance issues. 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.

  The number of allowed concurrent users is always limited by the number of licensed users. This number is capped by the Maximum Allowed Users in case the number of licensed users is greater than the number of Maximum Allowed Users.

- External Domain Url

  Defines the external URL of the DIVA View server such that password recovery links can be used from outside the network. The primary function of the External Domain URL is to define a registered certificate with a hostname so a custom web address can be supplied to users within the network. This has nothing to do with the password recovery links; those are configured on the Customer page with the SMTP configuration.

Note: The Client Uploader is no longer supported starting with release 6.0.

Company Logo

The following field is configurable in the Company Logo area of the screen:

- Company Logo Image

  Use the Browse button to select a company logo to display on the top of the DIVA View screen (if desired).

System-Wide Messages

Administrators can send messages to everyone on the system using the System-Wide Message function on the System Settings page. Messages can be an Announcement, Warning, or Alert. Use the pull-down list to select the type of message to send, enter your message into the Message text area, and press ENTER to send the message.

System Maintenance Settings

The System Maintenance options are located under Administrator > System Management > System Maintenance; changes made on this page are applied after you click Save:

The pull down menus for the Delete Inactive Objects and Delete Inactive Proxies include the following options:

- Do Not Delete

  Do not delete inactive objects

- Delete On Next Task

  Delete inactive objects when the next task is executed.

- Delete On Every Task

  Delete inactive objects every time a task is executed.

Housekeeper File Management Settings

Housekeeper is a running task incorporated into the TaskManager Service that takes care of DIVA View Server functional cleaning. It is scheduled as per the parameters listed under the House Keeper Scheduling section of the System Maintenance screen. When it runs, the logs are available into the taskmanager logs folder.

The following fields are configurable in the Housekeeper File Management Settings area of the screen:

- Local Request Files

  Defines the number of days to keep the files that have been restored to the DIVA View Server host computer through all local request operations. Cleanup is for Restore operations only. These are the downloadable files presented in the Operation Status page when a Local Restore is performed.

- DIVA Core Request Status

  Defines the number of days to keep the DIVA Core status information on the Operation Status screen.

- Audit Trail

  Defines the number of days to keep the audit trail.

- System Logs

  Defines the retention policy for all DIVA View logs.

- Scheduled Backups

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

- Shot Lists

  Defines the number of days (or forever) to keep Shot Lists.

telestream

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. This parameter is set to Do Not Pre-Cache by default to leave maximum memory for the server.

  Pre-caching can greatly increase the performance of the site on systems containing a lot of memory. This allows Postgres to hold commonly used tables in memory, which results in faster database requests.

Synchronization Maintenance Flags

The following fields are accessible in Synchronization Maintenance Flags area of the screen. These parameters are the cleanup housekeeping used in conjunction with the DIVA Core Synchronization (see *DIVA Core Synchronization*):

- Delete Inactive Objects

  Click this Trash Can icon to notify the Housekeeper to permanently delete objects marked as Inactive by the synchronization process. Proxies and binary files associated with deleted objects are moved to the deleted folder in their respective proxy storage location. See the following *Deleting Inactive Objects* section for details on deleting inactive objects.

- Delete Inactive Proxies

  Click this Trash Can icon to notify the housekeeper to permanently delete all files contained within the deleted folders on each proxy storage location. Deletion takes place during the next Housekeeping execution.

The pull down menus for the Delete Inactive Objects and Delete Inactive Proxies include the following options:

- Do Not Delete

  Do not delete inactive objects

- Delete On Next Task

  Delete inactive objects when the next task is executed.

- Delete On Every Task

  Delete inactive objects every time a task is executed.

Deleted Object Restoration

Deleted objects can now be restored. This enables recovery of mistakenly deleted objects from DIVA Core. Use the following procedure to restore deleted objects:

1. Use the search text box to quickly locate the deleted object to be restored.

2. Select the object, or objects, to restore from the list in the text area. Hold the CTRL key and click on multiple objects to restore, or hold the SHIFT key and click on the starting object, then the ending object, to select multiple files as an inclusive group.

3. After selecting the desired objects, click the right arrow to add them to the text area to the right of the list text area.

4. When all desired objects have been identified and added to the right text area, click Restore to restore the objects to Virtual Objects.

Housekeeper Scheduling

The following fields are configurable in Housekeeper Scheduling area of the screen:

- Last Run Date

  This non-configurable field displays the last date and time the Housekeeper tasks were run.

- Next Run Date

  This non-configurable field displays the next date and time the Housekeeper tasks are scheduled to be executed.

- Periodicity

  Use the drop down menu to select the period to run the Housekeeper tasks. The available options are as follows:

  – Daily

    Select this option to run the Housekeeper tasks daily.

  – DaysOfWeek

    Select this option to assign specific days of the week to run the Housekeeper tasks. When selected, a list of the days of the week is displayed. Select the check box for each day the tasks should be executed and deselect the check box for each day the tasks should not be executed.

  – Weekly

    Select this option to run the Housekeeper tasks once per week. When selected, the option to select which day to run the tasks is displayed on an additional drop down list; select the desired day of the week to run the tasks.

  – BiWeekly

    Select this option to run the Housekeeper tasks every other week. When selected, the option to select which day to run the tasks is displayed with an

additional drop down list; select the desired day of the week to run the tasks.

– Time of Day

Enter the time of day for the Housekeeper tasks to be executed in the text box. Alternatively, click the Clock icon to display a Time Picker and select a hour to run the tasks from the available choices.

telestream

DIVA Core Synchronization

The System Synchronization page is accessible from the Administration >System Management > DIVA Core Synchronization menu. This page displays synchronization tasks and links for downloadable logs for each task execution.
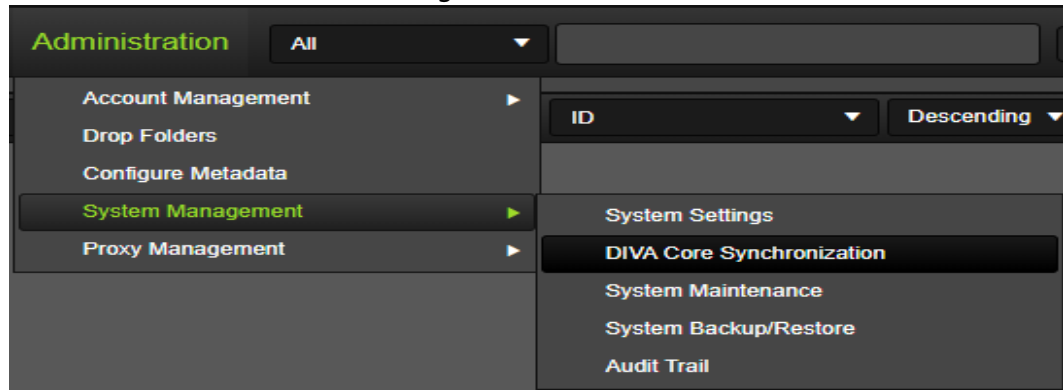
The following figure shows the DIVA Core Synchronization tasks screen (this is a partial screen shot). This is the screen displayed when you first access the DIVA Core Synchronization menu item.

Use the following procedure to configure the synchronization options:

1. Navigate to the DIVA Core Synchronization screen under the Administration > System Management pull down list.

2. Click the Show Scheduling button on the top right of the screen to display options for configuration of frequency and size of synchronization actions between DIVA View and DIVA Core.

telestream
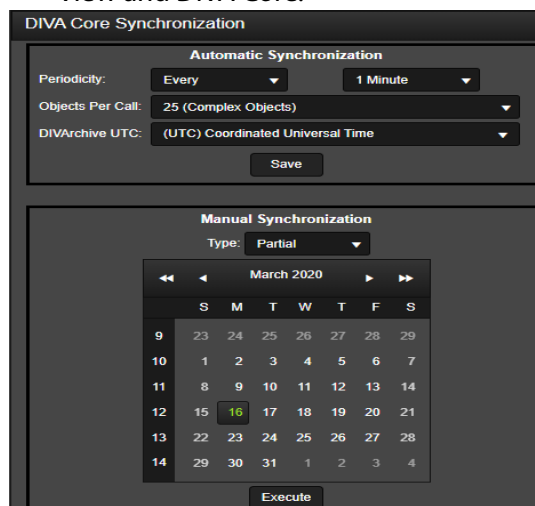
Automatic Synchronization

Synchronization scheduling is done in the Automatic Synchronization section of the screen. The following configuration options are available for automatic synchronization:

- Periodicity

  Use the left pull down list to select Every, Daily or Weekly. Then select the time period (for Every), time of day (for Daily), or day of the week (for Weekly) to execute the synchronization from the pull down list to the right of this list.

- Objects Per Call

  Use the pull down list to select the number of objects to include in each synchronization call.

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.

- DIVA Core UTC

  Use the pull down list to select the time zone where the DIVA Core system is located.

When your selections are complete click Save to save your Automatic Synchronization configuration.

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 Technical 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. Use the calendar displayed to select the start of the partial synchronization.

- 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 DIVA Core 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.

Deleting Inactive Objects

Inactive Objects will not show up in search results and can be deleted. During synchronization the following process occurs:

1. The object status is identified to determine if the object exists in DIVA Core.

2. When a Delete request is sent from DIVA View, if the Virtual Object is fully deleted from DIVA View. If it is not a virtual object, there is no change to the object immediately; this is in case the delete fails after submission during processing.

3. The object is marked as inactive during the next synchronization with DIVA Core.

4. The object is completely removed from the system if the Housekeeping Delete Inactive Object flag is set.

Synchronization Filtering

Synchronization filters define which objects are processed during synchronization. Each synchronization filter represents a combination of an object's parameters including Object Name, Object Collection 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.

+	Synchronization Filters			
	Object Name	Object Category	Media Name	Enabled
✏	chee*	Composites	*	☑	✗

Note: 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 DIVA View has already been synchronized and you 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.

As seen in the following figure, you can see the number of objects in each state on the bottom of the main screens.

Active Objects: 3 | External Objects: 0 | Inactive Objects: 0 | Synchronizing Objects: 0 | Virtual Objects: 3

Automated Backup Configuration

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

Use the following procedure to configure your automated backups:

1. Navigate to Administration > System Management > System Backup.
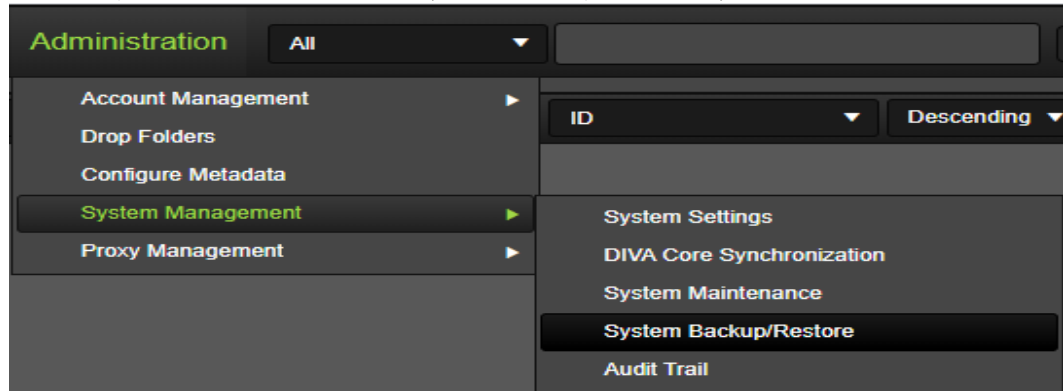
2. The following screen is displayed including configuration options and previous backup listings.

Filename	Size
DIVAdirector_database_20200311-0000.sql	32.89 MB
DIVAdirector_database_20200312-0000.sql	33.25 MB
DIVAdirector_database_20200313-0000.sql	33.66 MB
DIVAdirector_database_20200314-0000.sql	34.02 MB
DIVAdirector_database_20200315-0000.sql	34.38 MB
DIVAdirector_database_20200316-0000.sql	34.75 MB
DIVAdirector_database_20200317-0000.sql	35.28 MB
DIVAdirector_database_20200318-0000.sql	35.84 MB

3. Select the Enable Backup Schedule check box to enable the backup schedule.

4. Use the Periodicity list to select either Daily, DaysOfWeek, Weekly or BiWeekly backup frequency.

   If the Periodicity is set to Daily the backup will run every day at the scheduled time.

   If the Periodicity is set to DaysOfWeek, 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. The backup will run during the selected day(s) at the scheduled time.

   If the Periodicity is set to Weekly, you can select the day to run the backup using the pull down list for Week Day.

   If the Periodicity is set to BiWeekly, you can select the day to run the backup using the pull down list for Week Day.

5. 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)

6. 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 DIVA View scheduled backup task will be triggered accordingly by the TaskManager. See *Housekeeper File Management Settings* for information on the number of days to keep backup files.

The initial configuration of DIVA View is now complete. In the next chapter you will find Watch Folder Configuration.

telestream

Configuring DIVA View Web Server

DIVA View uses IIS (Microsoft Internet Information Server) 8 as the web server engine. Windows server requires IIS to be installed separately.

The DIVA View 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 Technical 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, DIVA View 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 DIVA View 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 DIVA View installation process creates an account named dd6-user. Technical Support recommends that you run IIS using a domain account. This is only true if a domain account is not provided during installation. If you need to do this after installation has occurred, the user must be added to the IIS_USRS group for the App Pool to run. Adjusting this is not in an obvious location. Navigate to AppPools > DV6 App Pool > Advanced Settings > Identity to make the necessary adjustments.

Next you will configure accounts.

Account Configuration and Management

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 DIVA View 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, configure a new organization.

Adding or Editing 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 DIVA View.

Navigate to Administration > Account Management > Configure Organization from the top main menu bar. The following screen is displayed:
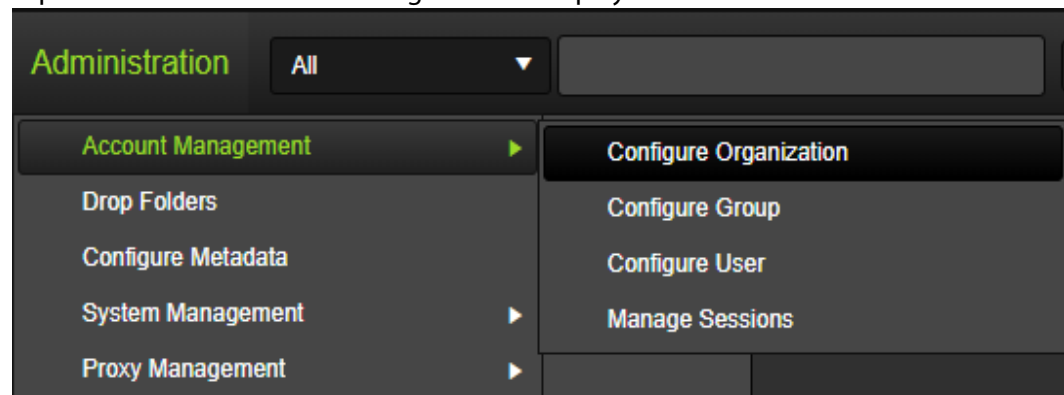
Configure the new organization, or edit an existing organization, General settings as desired using the following options:

Customer Profile

Organization

Use the pull down list to select an existing organization to edit or New Organization to create a new one.

Note: The System organization cannot be deleted. This is a default organization that includes the System Administrator account.

Organization Name

Enter the organization name in the text box when creating a new organization. The organization name will appear in the text box automatically when editing an existing organization.

LDAP Settings

- Enable LDAP Login

  Select the check box to enable LDAP logins. Hovering over the LDAP URL text box displays allowable formats as follows (if no port is specified the default LDAP port is used):

  ```
  ldap://172.0.0.1:636
  ldap://domain.com/
  ldap://domain.com:1234/ou=foo,dc=domain,dc=com
  ```

- Primary IP Address

  Enter the primary IP address in the text box. If the Enable LDAP Login check box is deselected this field is not accessible.

- Secondary IP Address

  Enter the secondary IP address in the text box. If the Enable LDAP Login check box is deselected this field is not accessible.

SMTP Email Configuration

Note: To enable SMTP email notifications, or for the user to receive a valid password reset link in the email sent when a password reset is requested, you must enter a valid external domain URL on the System Settings page (under the Administration menu) in the External Domain URL text box.

- Enable Email Notifications

  Select the check box to enable email notifications for the organization; otherwise leave it deselected. Email notifications are needed to receive an email requesting a password reset in the case of login failures.

- SMTP Server Address

  Enter the SMTP Server IP address in the text box. If the Enable Email Notifications check box is deselected this field is not accessible.

- SMTP Server Port

  Enter the SMTP Server port number in the text box. For non-SSL connections this is typically port 25; for SSL connections this is typically port 485 or 587. Check with your Network Administrator to confirm the specific port number and whether to use a SSL connection. If the Enable Email Notifications check box is deselected this field is not accessible.

- Enable SSL

  Select the check box to enable SSL secure connections to the SMTP server. If the Enable Email Notifications check box is deselected this field is not accessible.

- SMTP User Name

  Enter the SMTP username in the text box. If the Enable Email Notifications check box is deselected this field is not accessible.

telestream

- SMTP Password

    Enter the SMTP user password in the text box. If the Enable Email Notifications check box is deselected this field is not accessible.

Content Filter

The following wildcards apply to the content filtering fields:

- Use an asterisk (*) to match any pattern

    Using a lone asterisk in this field is invalid because it would match everything and serve no realistic purpose.

- Use a semicolon (;) to delimit a list

- Use and exclamation point (!) at the start of the filter criteria to indicate the filter is inclusive

Examples:

The following will be interpreted to include all collections that start with Test except for Test2.

`!Test*;Test2`

The following will be interpreted to include everything except the Test1 and Test2 collections

`Test1;Test2`

- Object

    Enter the objects available to this organization in the text box.

- Category

    Enter the collections available to the organization in the text box.

- Site

    Enter the site names available to the organization in the text box.

Metadata Access

Select the check box for each metadata field to include access to it in the organization; deselect the check box for any fields you do not want accessible by the organization. This allows creating Metadata lists where only the Organization being granted access to certain User Metadata will be able to view, search, and display that Metadata.

Configure the new organization, or edit an existing organization, DIVA Core Settings as desired using the following options:

- Unmanaged Storage Repository Access

  Select the check box for each Server the organization should have access to, or deselect any check box the organization should not have access to.

- Storage Plan Access

  Select the check box for each Storage Plan the organization should have access to, or deselect any check box the organization should not have access to.

- Media Access

  Select the check box for each Media the organization should have access to, or deselect any check box the organization should not have access to.

Click Save on the top right of the screen to save the changes or updates to the organization.

Note: If the DIVA Core Settings page is empty, it indicates that DIVA View is not connected to Core. See *DIVA View API Service* for information on connecting the API.

Adding or Editing 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.

Navigate to Administration > Account Management > Configure Group from the top main menu bar. The following screen is displayed:
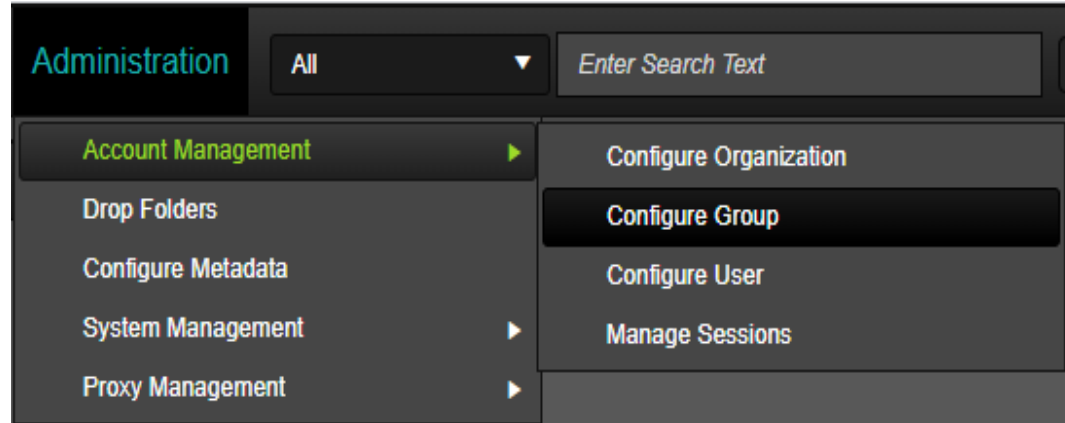
Select the group to work on from the Group pull down list at the top.

Group Profile

Configure the new group, or edit an existing group, Profile as desired using the following options:
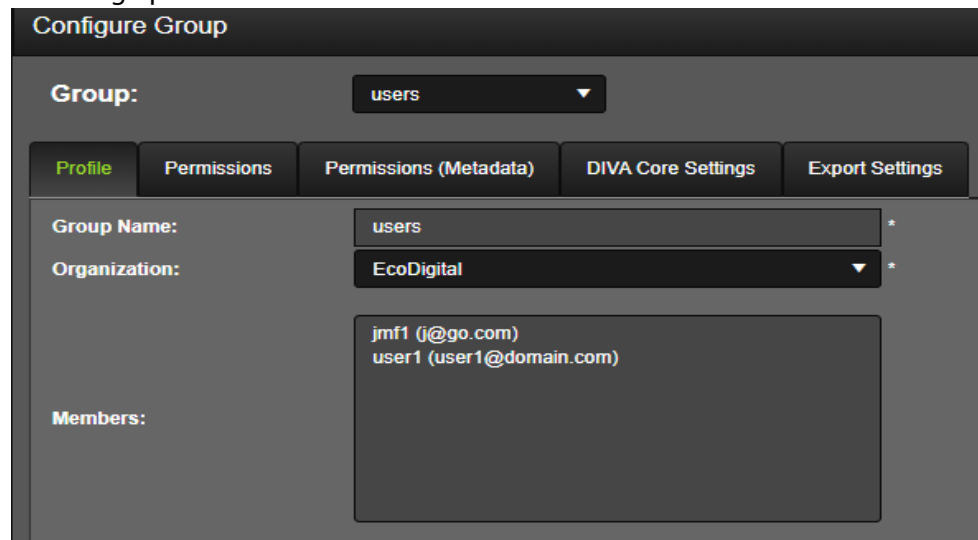
- Group Name

  Enter or edit the name of the group in the text box.

- Organization

  Use the pull down list to assign this group to an existing organization.

- Members

  This text area is non-editable and displays all of the users assigned to this group including their email addresses (blacked out in the previous figure).

Group Permissions

Configure the new group, or edit an existing group, Permissions as desired using the following options:

- **Privileges Area**

  Select the check box for each permission the group should have; otherwise leave the check box deselected. Selecting the top check box next to General, DIVA Core Operations, or Administration will select all permissions under that heading.

  – **General:**

    You can enable or disable the following permissions using the check boxes next to each item.

    * Create and View Searches

      Select the check box to enable creating and viewing searches for the group members; otherwise leave it deselected.

* Create and View Work Bins

  Select the check box to enable creating and viewing Work Bins for the group members; otherwise leave it deselected.

* Create and View Shot Lists

  Select the check box to enable creating and viewing Shot Lists for the group members; otherwise leave it deselected.

* Modify Metadata

  Select the check box to enable modifying metadata for the group members; otherwise leave it deselected.

* DIVA Core Site Information

  Select the check box to enable viewing DIVA Core Site Information for the group members; otherwise leave it deselected.

* View Proxies

  Select the check box to enable viewing Proxies for the group members; otherwise leave it deselected.

* Proxy Upload and Generation

  Select the check box to enable uploading and generating Proxies for the group members; otherwise leave it deselected.

* Download Proxies

  Select the check box to enable downloading Proxies for the group members; otherwise leave it deselected.

– **DIVA Core Operations:**

  You can enable or disable the following permissions using the check boxes next to each item.

  * Archive

    Select the check box to enable archiving DIVA Core objects for the group members; otherwise leave it deselected.

  * Delete

    Select the check box to enable deleting DIVA Core objects for the group members; otherwise leave it deselected.

  * Restore

    Select the check box to enable restoring DIVA Core objects for the group members; otherwise leave it deselected.

  * Partial Restore

    Select the check box to enable Partial Restore of DIVA Core objects for the group members; otherwise leave it deselected.

  * Use only Group DIVACore Request Profiles

    Selecting the Use Only Group DIVACore Request Profiles check box will restrict users of this group to only using the Request Profiles you have established.

* Download Restore

    Select the check box to enable downloading restored DIVA Core objects for the group members; otherwise leave it deselected.

– **Administration:**

You can enable or disable the following permissions using the check boxes next to each item.

* System Administration

    Select the check box to enable System Administration for the group members; otherwise leave it deselected.

* Proxy Administration

    Select the check box to enable Proxy Administration for the group members; otherwise leave it deselected.

* Session Management

    Select the check box to enable Session Management for the group members; otherwise leave it deselected.

* User Management

    Select the check box to enable User Management for the group members; otherwise leave it deselected.

* Modify Metadata Schema

    Select the check box to enable modification of Metadata Schema for the group members; otherwise leave it deselected.

* Access All Groups in Organization

    Select the check box to enable accessing all groups within the organization for the group members; otherwise leave it deselected.

* Access All users In Group

    Select the check box to enable accessing all users within the group for the group members; otherwise leave it deselected.

* **Filter Area:**

    The following wildcards apply to the content filter fields:

    – Use an asterisk (*) to match any pattern

    – Use a semicolon (;) to delimit a list

    – Start the filter criteria with an exclamation point to indicate the filter is inclusive.

    The content filter fields are as follows:

* Object

    Enter the objects available to this group in the text box.

* Category

    Enter the collections available to the group in the text box.

* Site

    Enter the site names available to the group in the text box.

Group Permissions (Metadata)

Configure the new group, or edit an existing group, Permissions (Metadata) as desired using the following options. The following figure is a partial screen shot. Use the scroll bar on the right of the list to see all Metadata Permissions for the Group.
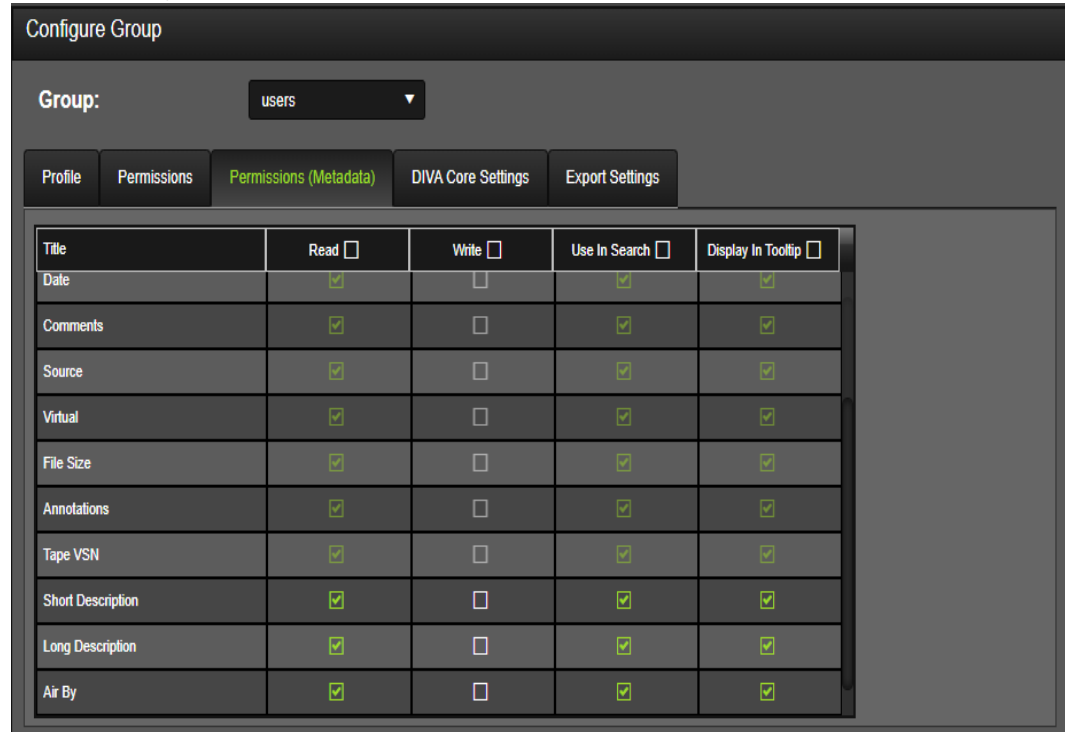
Some of the options on this screen are system settings and cannot be changed. Those check boxes are lighter in color or grayed out in the previous figure. All other options can be applied by selecting the check boxes on the option's row.

The column headers on this screen are self-explanatory. For example, if you want to allow users of the group to have Read permission for certain metadata, select the check box under the Read column for each metadata you want the group to be able to view. If you leave the check box deselected the users of the group will not have access to that metadata.

Another example is that if you want to give permission to write to the metadata field, select the check box under the Write column for that metadata field and users of the group will be able to enter information in that field.

Selecting the check box next to the column header will provide users of the group with that specific permission for all metadata fields in the column. The displayed Metadata is the Metadata that the Organization has permission to access. If there are User Metadata fields that are not seen in the Group, you must enable it in the Organization settings.

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 Configure Group 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 DIVA View User's Guide for more information on publishing).

Annotation Templates

Annotation templates are preconfigured annotations that can be added to a file and then modified to where they occur in a clip. They are configured in the Configure Metadata page.
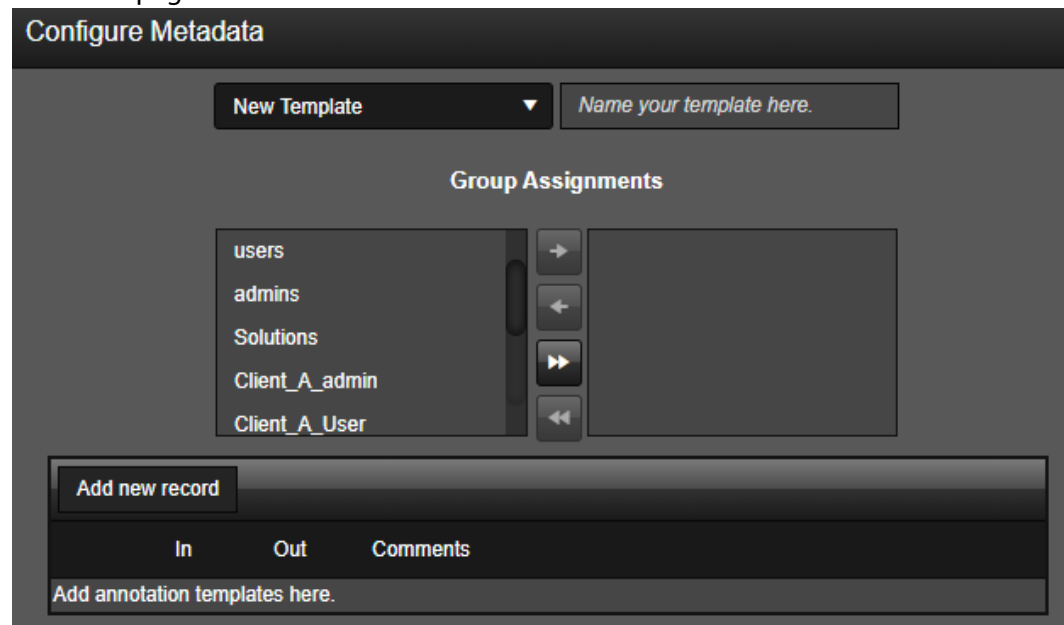
Use the following procedure to create an Annotation Template:

1. Navigate to Administration > Configure Metadata.

2. Use the pull down menu on the top right of the page to select Annotation Templates.

3. Enter a name for the template in the Name your template here text box.

4. Select the groups this template is assigned to under Group Assignments. Highlight the groups on the left side and click the right arrow in the middle to add the group. You can add all displayed groups using the right-facing double arrow in the middle.

5. Click Add new record on the Add annotation templates here area; the following screen is displayed.

6. Enter the In Time, Out Time and any Comments in the appropriate fields.

7. Click Insert to add the template.

8. Click Save on the top right of the screen to save the new template.

telestream

Select an existing template from the pull down list at the top and click Delete on the top right of the screen to delete a template.

Select an existing template from the pull down list at the top to edit an existing template, then click Save on the top right of the screen to save the changes.

telestream

Group DIVA Core Settings

Configure the new group, or edit an existing group, access to DIVA Core functions using the checkboxes on this page in each section of the page.

- **Archive Area**

    The following subsections are available. Select the check box for each item to give access to that item for the Group; otherwise leave it deselected. The following is a partial screen shot of the page; scroll down to access the additional functionality settings.

- **Source**

  Select the sources the group should have access to in DIVA Core.

- **Media**

  Select the media the group should have access to in DIVA Core.

- **Storage Plan**

  Select the storage plans the group should have access to in DIVA Core.

- **QoS**

  Select the Quality of Service level from the pull down menu that the group should have access to in DIVA Core.

- **Priority**

  Enter the job priority the group should have access to in DIVA Core. Alternatively use the scroll buttons to change the value.

- **Category**

  Select the collections the group should have access to in DIVA Core. You can add collections using the + icon on the top of this section. You can remove collections using the red X icon on each row. The collections in the Archive configuration refers to the available options for a user to archive to. These do not have anything to do with which collections a group can see. This list is also shared with the Virtual Object creation. Both pages will show a warning when no Archive collections are added for a given group.

  * Force default value

    Select the check box to force use of the default values in each of the previous subsections; otherwise leave it deselected.

- **Delete Area**

  Enter the job priority for Delete jobs or use the scroll buttons to change the value. Select the Force default value check box to enable this function; otherwise leave it deselected.

telestream

- **Partial Restore Area**

  The following subsections are available. Select the check box for each item to give access to that item for the Group; otherwise leave it deselected.

  – **Destination**

    Select the Destination Servers the group should have access to in DIVA Core.

  – **QoS**

    Select the Quality of Service level from the pull down menu that the group should have access to in DIVA Core.

  – **Priority**

    Enter the job priority the group should have access to in DIVA Core. Alternatively use the scroll buttons to change the value.

  – **File Format**

    Select the file format (or Autodetect) from the pull down menu that the group should have access to in DIVA Core. Technical Support recommends using Autodetect unless you are working with very old formats like SeaChange.

  – **PFR Name Format**

    Select the filename format from the pull down menu that the group should have access to in DIVA Core. There are two pull down menus. The first selects the separator (dash, period or underline), and the second selects the maximum length of the filename. Select the Use Relative TC check box to use relative time codes; otherwise leave it deselected.

  – **Force default value**

    Select the check box to force use of the default values in each of the previous subsections; otherwise leave it deselected.

- **Restore Area**

  The following subsections are available. Select the check box for each item to give access to that item for the Group; otherwise leave it deselected.

- – **Destination**

  Select the Destination Servers the group should have access to in DIVA Core.

- – **QoS**

  Select the Quality of Service level from the pull down menu that the group should have access to in DIVA Core.

- – **Priority**

  Enter the job priority the group should have access to in DIVA Core. Alternatively use the scroll buttons to change the value.

- – **Force default value**

  Select the check box to force use of the default values in each of the previous subsections; otherwise leave it deselected.

Publish Profile Settings

Configure the DIVA Core Publishing Profile settings on the Group Configuration page using the following procedure:

1. Click the DIVA Core Settings tab.

2. On the top right click Show Profiles.

3. If no profiles have been configured yet, click the red + to configure a new profile. If there are existing profiles, select the profile to update and the parameters for that profile appear.

4. Use the pull down menu to select the Publish Profile for this group. All users in the group will have the same Publish Profile setting.

5. Repeat the process for all profiles requiring updating.

6. Click Save on the top right of the screen to save the changes.

Group Export Settings

Configure the new group, or edit an existing group, Export Settings as desired using the following options:

Use the pull down lists to configure the group Export Settings. The available options are as follows:

- Default Shot List Export Video Format

  Use the pull down list to select one of the following options:

  – PAL

    This is the format used mainly in Europe.

  – NTSC

    This is the format mainly used in the North America, South America and Japan.

- Default Shot List Export Format

  Use the pull down list to select one of the following options:

  – Final Cut Pro

    This is the Apple video editing software.

  – Avid ALE

    This is the Avid video editing software.

- Default Metadata Export Format

  Use the pull down list to select one of the following options:

  – CSV

    This is the Comma Separated Values format and can be opened in a plain text editor or as an Excel spreadsheet.

  – XML

    This is the eXtensible Markup Language format and can be opened in a plain text editor or software such as Notepad++.

Adding or Editing a User

All users are members of a group and inherit the roles and accesses assigned to the group. You add new users, or edit existing users, using the following procedure:

Navigate to Administration > Account Management > Configure User from the top main menu bar. The following screen is displayed:
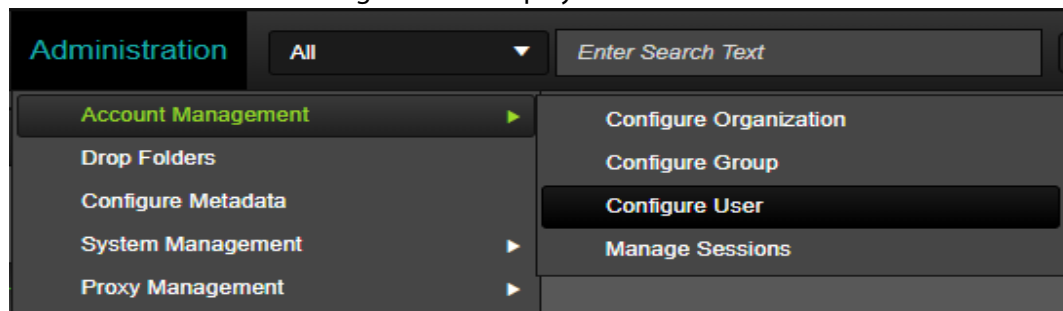
Configure the new user or edit an existing user as desired using the following options. Fields with an asterisk (*) at the end of the row are required fields.

Account Information

You configure basic account information in this section, which includes the following fields:

- User Name

  Enter the desired username to use for logging into the system. This is a required field.

- Group

  Use the pull down list to select the Group the user should be a member of. This is a required field.

- Email

  Enter the user email in the text box. This is a required field.

- Lockout Status

  Use the pull down list to select the Lockout Status of this user. The following options are available:

  – Not Locked

    The user has access to the system.

  – Locked

    The user does not have access to the system.

  – Locked By An Administrator

    A System Administrator has locked the user out of the system.

  – Temporary Password

    Enter a temporary password for a new user, or update the password for an existing user in the text box. This is a required field and follows the requirements for the Administrator password.

Note: All passwords are case-sensitive. There are rules for passwords as follows:

All passwords have a 3 month forced expiration. This cannot be modified.

Must be between 8 and 128 characters

Must contain a letter

Must contain a number

Must contain a symbol

Must not contain whitespace characters

New password must not be a previously used password.

---

telestream

- Confirm Password

  Confirm the password you entered in the previous field. See the previous note on password requirements. This is a required field.

- Display page on user login

  Use the pull down list to select the page the user will see when they log into DIVA View. Options include the following:

  – Introduction Page

  – Most Recent Query

  – Last Page Accessed

  – Active Query

  – Active Work Bin

  – Active Shot List

Personal Information

You configure the personal user information specific to this user in this section, which includes the following fields (that are not required). These fields can be left blank if you want the user to enter their own information after they login, or if your company does not require the information for DIVA View.

- First Name

  Enter the user's first name in this text box.

- Last Name

  Enter the user's last name in this text box.

- Street

  Enter the user's street address in this text box.

- City

  Enter the user's city in this text box.

- State/Province

  Enter the user's state or province in this text box.

- Zip

  Enter the zip code for the state or province in this text box.

- Country

  Enter the user's country in this text box.

- Telephone

  Enter the user's telephone number in this text box.

- Cell Phone

  Enter the user's cell phone number in this text box if applicable.

telestream

- Fax

    Enter the user's fax number in this text box if applicable.

Click Save on the top right of the screen to save the new or updated user.

Session Management

This section describes managing user sessions.

Navigate to Administration > Account Management > Manage Sessions from the top main menu bar. You set the Session Timeout parameter in the configuration file located at C:\Program Files (x86)\EcoDigital\DIVAView\www\Web.config under the system.web section as follows (timeout is in minutes):

```
system.web
<sessionPageState <other fields> timeout="xxx"/>
```
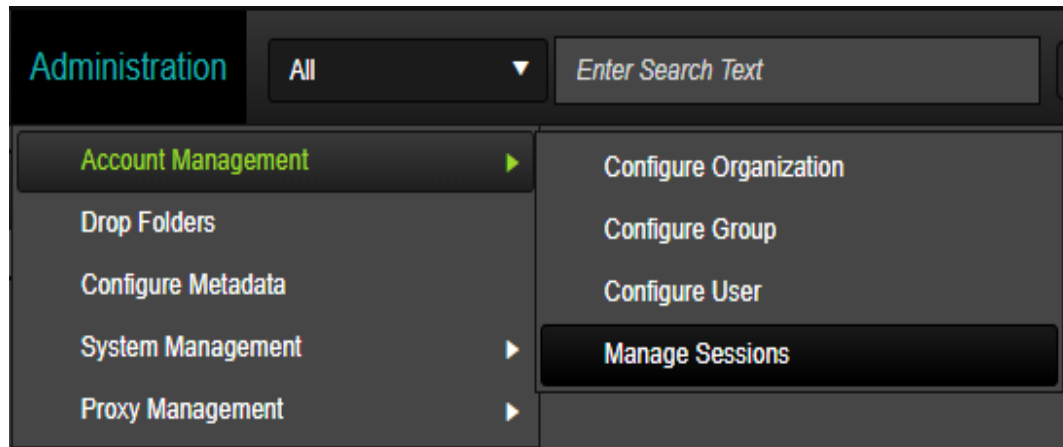

The top section of the screen displays the DIVA View license information and is non-editable. The following figure is a partial screen shot.
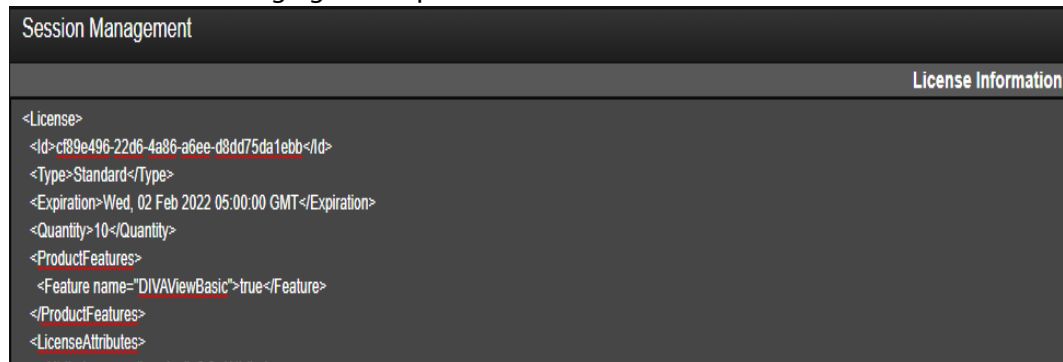
The center section of the screen displays users who are currently logged into DIVA View. The following figure is a partial screen shot.

Right-click on an active user to display a context menu allowing you to Refresh the screen, or Sign out user.
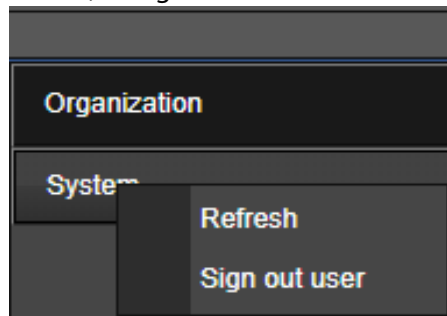
The bottom section of the screen displays offline users and additional information about the user. The following figure is a partial screen shot.

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 Administration > System Management > System Settings screen.
2. Select the type of message from the Type pull down list.
3. Enter the message text in the Message text area.
4. Click Save on the top right side of the screen to save the message.

Metadata Configuration

Metadata is used in system wide searches on the DIVA View and DIVA Core systems to locate a specific file, Collection of files, objects, or video clips. These roles are set for the Organizations and Groups and apply to all members of the Organization and Group.

See the sections on *Adding or Editing an Organization*, and *Adding or Editing a Group* for information on adding metadata permissions for Organizations and Groups.

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 DIVA Core (OBJECT_NAME, OBJECT_CATEGORY, ARCHIVE_DATE, and so on).

The Object Metadata screen is accessible from the Administration > Configure Metadata screen:
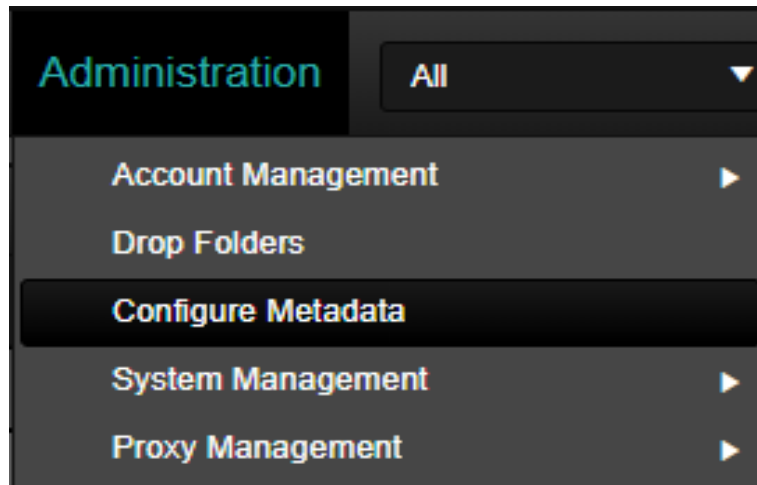
The following screen is displayed (this is a partial screen shot):

Title	Type	Format	Description
ID	Number	EditBox	Object ID
Name	String	EditBox	Object name
Category	String	EditBox	Object category
Date	Date	Calendar	Archiving date
Comments	String	TextBox	Object comments

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

  DIVA View defined unique identifier for the object.

- Name

  DIVA Core system defined Object Name used as a unique identifier with the Collection.

- Category

  DIVA Core system defined Object Collection used with the name.

- Date

  The date when the object was archived to the DIVA Core 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.

The metadata fields at the top of the screen is system generated and cannot be edited. Any editable metadata fields will have a Pencil icon next to them for editing. Use the following procedure to add new metadata fields:

Note: The following procedure is an example using the String Type. Other Types will have additional fields to configure.

1. Click + on the top left of the screen to add new metadata for objects in DIVA View. The following screen is displayed:

2. Enter the metadata name in the Title text box.

3. Select the metadata type to be added from the Type pull down list.

***

Note: See *Data Types* for a description of the different Data Types available in the pull down menu.

***

4. Select the format (TextBox, EditBox, and so on) from the Format pull down list.

5. Enter a description for the metadata in the Description text area.

6. Enter the maximum length for the field in the Length text box. Alternatively, you can use the up and down arrows attached to the text box.

7. Enter YES or NO in the Default text box to identify whether the metadata is a default.

8. Is the metadata is to be hidden, select the check box next to Hidden (Hid).

9. Click the green Check to save the changes, or the red X to cancel them.

You can change any metadata field from not hidden to hidden (and vice versa) using the check box on the right side of the metadata row.

To delete any non-system metadata, open the metadata field by clicking the Pencil icon and then click Delete on the top right of the screen.

Data Types

DIVA View 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 - 1000 characters in length. The String data type can be represented using an EditBox, TextBox, or SelectBox control (refer to *DIVA View Presentation Controls*).

telestream

- Number

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

- Decimal

  Any numeric value - including decimals. The Decimal data type can be represented using an EditBox or check box 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 SAMMAsolo. 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 (currently only Baton is implemented - other implementation are by request)
    - Selected (selected or deselected)
    - Data file extension
    - Report file extension

DIVA View Presentation Controls

Most metadata field data types have multiple ways of displaying data and some are restricted to using particular controls (these are limited by the type of metadata). 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.

telestream

- CheckBox

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

- Multi CheckBox

  Allows users to select multiple options by selecting the appropriate check boxes.

- 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 Storage 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 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.

Adding Quality Control Metadata

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

1. Click +Add on the top right side of the screen.

2. Enter a name for the metadata in the Title field.

3. Select qc report from the Type list.

4. Select QC Report from the Format list.

5. Select which reports should be visible using the check boxes next to each type of report.

6. Enter the data file extension (usually xml) for each visible report in the Data Extension field.

7. 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).

8. Enter a description in the Description field.

9. Select the Hidden (Hid) check box if you want the report hidden from users; otherwise, leave it deselected.

10. 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.

telestream

Metadata Column Manager

The Administration > Configure 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 DIVA Core and Proxy Metadata, are predefined, will be always present in the table, and cannot be deleted.

The order of the entries can be changed by dragging and dropping the row to another position to complete the repositioning. The ordering is done on a per-user basis for users who have access to this page. It is not a global reordering like it was in previous releases.

Select the Hidden check box to hide the entry from the Metadata screen; otherwise leave it deselected so it displays on the screen.

Editing a Metadata Entry

Use the following procedure to edit a Metadata Column:

1. Navigate to the Administration > Configure 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 green Check Mark icon to save the changes or click the red X icon to cancel the changes.

Deleting a Metadata Entry

Use the following procedure to delete a metadata entry:

1. Navigate to the Administration > Configure 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.

Configuring Metadata Profiles

One or more Metadata Profiles must be configured from the Administration > Configure Metadata screens. Use the following process to create a Metadata Profile:

1. Navigate to Administration > Configure Metadata.

2. Use the pull down menu on the top right of the screen to select the Metadata Publish Profiles item.
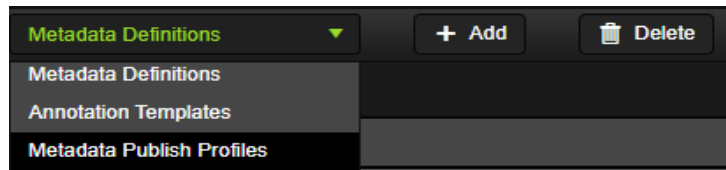
3. If there are existing profiles and a new profile is required, click + Add on the top right, or the red + icon (on the left) to add and configure a new profile. Go through the items on the page and configure the profile as required using the following necessary parameters:
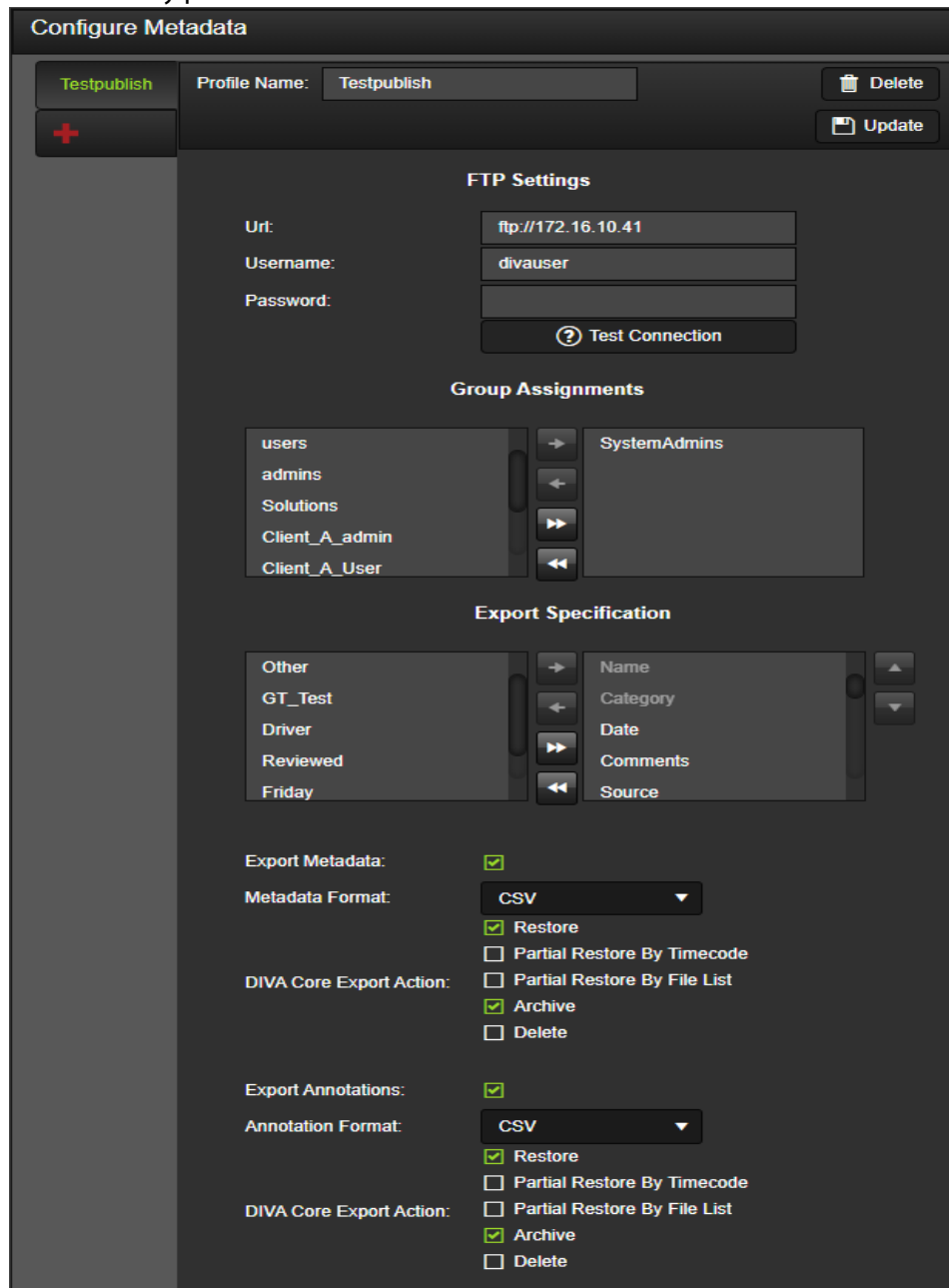
- **Profile Name**

  Enter a name for the profile in the text box.

- **FTP Settings**

  Enter the appropriate parameters in the text boxes as follows:

  – Url

    Enter the FTP server URL.

  – Username

    Enter the username to connect to the FTP server.

  – Password

    Enter the password for the username being used to connect to the FTP server.

  Click Test Connection to confirm the entered parameters are correct.

- **Group Assignments**

  Select the group to include in the profile from the left text area and then click the right-facing arrow to add it to the profile; use the double right-facing arrow to add all groups. To remove a group, select the group in the right text area and click the left-facing arrow; use the double left-facing arrow to remove all groups.

- **Export Specification**

  Select the export parameter to include in the profile from the left text area and then click the right-facing arrow to add it to the profile; use the double right-facing arrow to add all parameters. To remove a parameter, select the parameter in the right text area and click the left-facing arrow; use the double left-facing arrow to remove all parameters.

- **Export Metadata**

  Select the check box to enable exporting metadata for the profile; otherwise leave it deselected to disable exporting.

- **Metadata Format**

  Use the pull down menu to select either CSV or XML for the Metadata Format. This function is disabled unless Export Metadata is enabled.

- **DIVA Core Export Action**

  Select the check box for any export actions that must be enabled for the profile; otherwise leave them deselected to disable the action. This function is disabled unless Export Metadata is enabled.

- **Export Annotations**

  Select the check box to enable exporting annotations for the profile; otherwise leave it deselected to disable exporting.

- **Annotation Format**

  Use the pull down menu to select Final Cut Pro, Avid ALE, CSV or XML for the Annotation Format. This function is disabled unless the Export Annotations is enabled.

telestream

- **DIVA Core Export Action**

    Select the check box for any export actions that must be enabled for the profile; otherwise leave them deselected to disable the action. This function is disabled unless Export Annotations is enabled.

Quality Control (*QC*) Report Configuration

DIVA View supports integration with QC Reports from Interra Baton.

Note: Venera Rapid, Venera Pulsar, Tektronix Cerify, are also supported by request.

Report files should be placed in the path under the IIS DIVA View 6 Root Folder:

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

For example:

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

First create a folder for the QC reports, then 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 DIVAView QC Report virtual directory under the DIVA View 6 menu item.

2. Right-click the DIVA View QC Report folder, and then select Explore from the context menu.

3. Create a new folder with a specific Collection (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).

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.

Watch Folder Configuration

This chapter describes Watch Folder configuration after installation

Topics:

- Watch Folder Configuration
- Additional Metadata Watch Folder Configuration
- Additional DIVA Core Watch Folder Configuration
- Additional Annotation Watch Folder Configuration
- Additional Proxy Watch Folder Configuration

telestream

Watch Folder Configuration

Watch 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, Watch Folders bypass the need for navigating a UI and can aggregate similar work into one simple action.

DIVA View actively monitors each Watch Folder for new files on disk and also has a Web Interface you can use to drop files and folders. Watch Folders are monitored, and files processed by the TaskManager Service. A given Watch Folder's visibility in the Web Interface is configured on a per group basis. Through the interface you may view each Watch Folder task status and any associated logs. You can view a monitor for a Watch Folder by selecting the folder in the pull down menu and clicking Show Monitor. This allows administrators to download Watch Folder logs and view failures (see *Show Monitor / Show Configuration*).

All four types of Watch Folders available are configurable.

Navigate to Administration, Watch Folders from the top main menu bar.
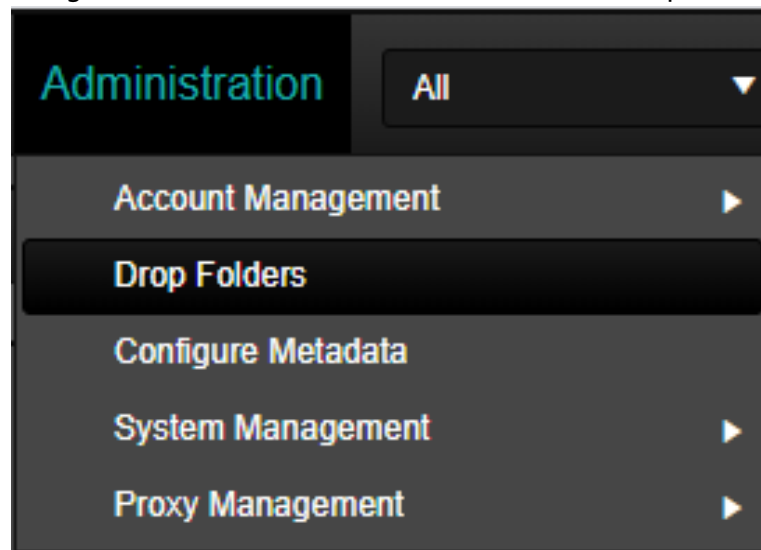
There are two buttons on the top right side of the screen. Click the Actions button to import an existing configuration. Click the Save button to save the new, or updated, configuration.

- Import

  Click Actions > Import and a file selector dialog box will initiate the Watch Folder configuration import process. Both legacy formatted Watch Folder configurations, and new XML 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.

- Save

  Clicking this button item saves the currently selected configuration.

telestream

Folder Settings

The following options are required and common to all Watch Folder Types:

- Watch Folder Type

  The type of Watch Folder dictates which configuration options are available. Use the drop down list to select the type of Watch Folder you are working on.

- Description

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

- Watch Path

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

- Log File Path

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

- Enabled

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

- Group Access

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

  If no groups are showing on the pull down list (and should be), or to add a group to the pull down list, use the pull down list under Add Group to select a group, then click Add. The selected group will now be displayed in the Group Access pull down list and given access to the Watch Folder. Repeat this process to add additional groups.

  To remove a group, select the group from the Group Access pull down list and then click Remove.

- Add Group

  This parameter is a list of available groups to assign to the Watch Folder. 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.

File Process Settings

The following options are required and common to all Watch Folder Types:

- File Format Type

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

telestream

- XML (Metadata Watch Folders only)

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

- CSV

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

- File Encoding

  This parameter identifies the configuration of the expected ingest files encoding. Use the pull down list to select the appropriate coding and confirm that the 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).

- Prevent Duplicate Files

  Select the check box to prevent duplicate files from being created. Leaving the check box deselected allows duplicate files to be created.

- Duplicate Path

  Enter the path where duplicate files will be saved in the text box.

- Duplicate Duration (seconds)

  Enter the number of seconds to allow for duplicate files to be created in the text box. If the creation takes longer than this number it will fail. If you are receiving constant failures, or multiple failures, increase this number to accommodate longer creation times.

CSV File Format Settings

The following options are required and common to all Watch Folder Types:

- Delimiter

  Importing CSV files supports using one of three delimiting characters; comma, semicolon, and tab. Use the pull down list to select the type of delimiter for this Watch Folder.

- Encapsulation

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

telestream

- 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 ignored by the parser.

- Show Monitor / Show Configuration

  Use the Administration > Watch Folders menu item to access the Watch Folder Create New Folder screen. When the screen displays, use the Create New Folder pull down menu and select the Proxy Watch Folders menu item. On the top right of the screen you can now select Show Monitor or Show Configuration (this is a toggle button).

  When Show Monitor is selected the screen displays the Watch Folder Monitoring screen that shows all Watch Folders and the state of the folder (includes submission time, file name, log file, progress, and so on).

  Clicking on Show Configuration displays the Watch Folder Configuration screen where you can edit an existing folder.

telestream

Additional Metadata Watch Folder Configuration

The following sections describe additional options for Metadata type Watch Folders only:

CSV File Format Settings

These parameters are located under the CSV File Format Settings section of the screen and are in addition to the common settings previously described.

- XML

  XML formatted metadata can be ingested provided the XML format guidelines are followed.

- Collection Matching (also for Proxy Watch Folders)

  This parameter enables matching a CSV row to objects without supplying a Collection within the dropped file.

Note: When a proxy Watch Folder is configured with this setting, the Watch Folder will assign the proxy based on a matched file name convention for objects that only contain one file. The CSV mode is used when legacy matching is disabled. When this is enabled the Watch Folder uses the file name to identify which object should be associated with the dropped proxy. XML has not been implemented for proxy Watch Folders. When using legacy mode, the object is located using the file name; otherwise the Collection is used.

Metadata Action Settings

These parameters are located under the Metadata Action Settings section on the right side of the screen and are in addition to the common settings previously described. These fields only appear for the Metadata type Watch Folder.

- Overwrite Existing Data

  Select this check box to enable overwriting existing data for the group; otherwise leave is deselected.

Caution: **Enabling this option can cause loss of data due to overwriting existing objects.**

- Delete Metadata on Null Field

  Select this check box to enable deleting metadata if there is a NULL field for the group; otherwise leave is deselected.

- Create Virtual Object

  Select this check box to enable creating virtual objects for the group; otherwise leave it deselected.

telestream

Field Mappings

These parameters are located under the Field Mappings section on the right side of the screen and are in addition to the settings previously described. These fields only appear for the Metadata and DIVA Core type Watch Folders.

Click Add to add a new metadata field mapping. Complete all configuration items and click Save to save the mapping. After you save the mapping it will appear in the Field Mappings list.

Additional DIVA Core Watch Folder Configuration

DIVA Core Watch Folders allow you to execute large numbers of DIVA Core jobs based on the folder configuration. The volume of jobs 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 Collection Matching settings previously described, a column defined for Object Collection may also be necessary.

Note: Multiple files can be archived simultaneously from a Watch Folder using a semi-colon (;) as a delimiter.

Use the Action pull down list under Folder Settings to determine the type of DIVA Core action to perform and the configurable options available. The types of actions are as follows:

- Archive

  This action encompasses all types of Archive actions.

- Copy

  This action enables the copying of assets to different media.

- Restore

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

- Purge

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

DIVA Core Request Processing Settings

The following settings are available under the DIVA Core Request Processing Settings on the right side of the screen.

- Max DIVA Core Queue Size

  This option sets the maximum number of active processing jobs before the Watch Folder will pause any new submissions. Use the pull down list to select from between 50 and up to 1000 active jobs.

- Request Set Size

  This option defines the number of jobs to send per sleep interval. Use the pull down list to select from between 5 and up to 100 jobs per Sleep Interval.

- Sleep Interval

  This option determines the length of time before sending new requests or checking the status of the DIVA Core processing queue. Use the pull down list to select from between 5 seconds and up to 10 minutes.

- Priority

  This option sets the priority level of jobs submitted to DIVA Core. Requests with higher priority take precedence over jobs with lower priority. Use the drop down list to select the job priority. This option can be overridden as part of the dropped CSV.

DIVA Core Request Settings

All of the following request settings can be overridden as part of the dropped CSV.

Archive and Restore Action Specific Options

The following options are available when you select the Archive Action type:

- Unmanaged Storage Repository

  Use the pull down list to select the originating Server of a request. You can provide specific credentials associated with the Source Server (Source Server Login and Password). You can also select the check box to enable deleting archived files after the job is processed.

- Media

  Use the pull down list to select the Media Name or Storage Plan for the archived asset.

- Quality of Service

  Use the pull down list to select the Quality of Service for the archive request. See the DIVA Core 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. Enter the desired Root Path in the text box.

- 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 object's metadata.

telestream

- Purge Action
  - Media

    This option identifies sets the media name to delete instances of an object from. This field is optional.
  - 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 Watch Folder Configuration
  - 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 Collection. 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 Watch 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.

Copy and Purge Action Specific Options

Selecting Copy from the Actions pull down list results in only the following option under the DIVA Core Request Settings. Other previously described options in this area will not be available.

- Media

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

telestream

Field Mappings

These parameters are located under the Field Mappings section on the right side of the screen and are in addition to the settings previously described. These fields only appear for the Metadata and DIVA Core type Watch Folders.

Click Add to add a new metadata field mapping. Complete all configuration items and click Save to save the mapping. After you save the mapping it will appear in the Field Mappings list.

Additional Annotation Watch Folder Configuration

Annotation Watch Folders allow the importation of commented segments for files within objects. The CSV files that are dropped with this type of folder use all of the common configuration options previously mentioned. See *Annotation Watch Folder Configuration and Log Files* for a sample configuration file.

Note: Unlike Metadata Watch Folders, existing entries for same Time Codes are not replaced.
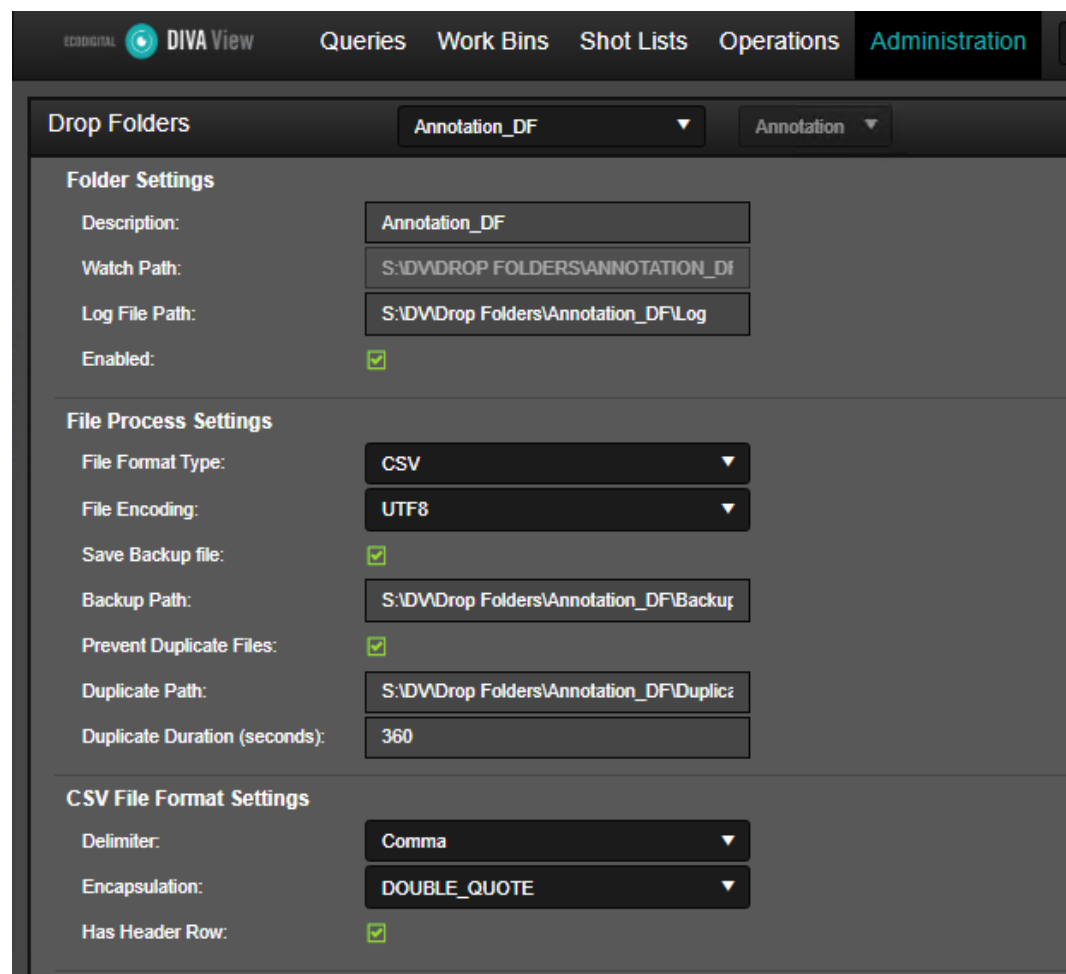
Use the following procedure to configure an Annotation Watch Folder:

1. Select Annotation from the pull down menu.

2. Enter your required parameter settings. The parameters fields are as follows:

   – **Folder Settings**

     * Description

       Enter a description for this configuration. When saved, this will populate the Watch Folder Name (to the left of the pull down menu). In the previous figure it is Annotation_DF; seen in both the Description and Watch Folder Name pull down box.

     * Watch Path

       Enter an appropriate path for this Watch Folder to watch for new files in the text box.

     * Log File Path

       Enter an appropriate path for the log file associated with this folder in the text box.

     * Enabled

       Select the check box to enable this configuration; otherwise leave it deselected.

   – **File Process Settings**

     * File Format Type

       Use the pull down menu to select the file format. In this case use CSV as shown in the previous figure.

     * File Encoding

       Use the pull down menu to select the file encoding format. In this case use UTF8 as shown in the previous figure.

     * Save Backup File

       Select the check box to enable saving a backup file; otherwise leave it deselected.

     * Backup Path

       Enter an appropriate backup path where backup files will be saved in the text box.

     * Prevent Duplicate Files

       Select the check box to enable preventing duplicate files from being created; otherwise leave it deselected to allow duplicate file creation.

     * Duplicate Path

       Enter an appropriate path for placement of duplicate files (if allowing duplicate file creation) in the text box.

     * Duplicate Duration (seconds)

       Enter the duration (in seconds) for duplicate file creation. If this number is exceeded the operation will timeout.

telestream

– **CSV File Format Settings**

Delimiter

Use the pull down menu to select the file delimiter. In this case it is Comma.

Encapsulation

Use the pull down menu to select the encapsulation setting. In this case it is DOUBLE_QUOTE.

Has Header Row

Select the check box if your CSV file has a header row; deselect it if there is no header row in the file.

3. Click Save on the top right to save the configuration.

Additional Proxy Watch Folder Configuration

Technical Support recommends using the transcode service rather than Proxy Watch Folders. Continued use of proxies produced outside of DIVA View and DIVA Core for local proxies will continue to function.

All proxies registered in the DIVA View system are kept on Proxy Storage Locations. These are configured in the Administration, Proxy Management, Proxy Storage Locations. By default, one proxy location is added during DIVA View installation. However, you can configure and manage multiple proxy storage locations. See *Proxy and Transcoder Configuration* for information on configuring 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\DIVAView\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.

Along with the common configuration fields previously describe in this chapter, the Proxy Watch Folder configuration screen enables configuration of the following options for each proxy location:

- Collection Matching

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

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

Proxy Watch Folder Manifest File Format

DIVA View associates proxies with files in an object, instead of the Virtual Object itself. It is also possible for multiple proxies to be associated with a single file. This is a new feature starting with DIVA View 6.0. To support this functionality, proxies dropped into a Proxy Watch 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, Collection, 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 Collection 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 DIVA View.

- 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, Collection, 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.

Thumbnails and Metadata

The following additional options are configured on the right side of the screen under the Thumbnails and Metadata section:

- Thumbnail Generation Workflow Name

  Use the pull down list to select the desired workflow for thumbnail generation.

telestream

Virtualization

The following additional options are configured on the right side of the screen under the Virtualization section:

- Enable File Virtualization

    Select the check box to enable creation of virtual files; otherwise leave it deselected.

- Virtual File Extension

    Enter the desired filename extension for virtual files in the text box.

Click Save to save the configuration.

Proxy and Transcoder Configuration

This chapter describes Transcoder configuration after installation.

Topics:
- Proxy Configuration
- Transcode Service Configuration

Proxy Configuration

The following sections describe the process for DIVA View transcoder configuration. See *Proxy Storage Structure Changes During Upgrades* for details on storage structure changes during upgrades.

Create Proxy Storage

Map the Storage Location in Windows and Set Folder Permissions

Use the following procedure 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 context 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 DIVA View 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 DIVA View Web Server.

Add the Proxy Folder to the DIVA View Web Server in IIS

Note: When editing anything in IIS, all users will be disconnected upon saving. Remember this and confirm there are no users on the system whenever any modifications are needed in IIS.

Use the following procedure to add the proxy folder to the DIVA View 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 DIVA View 6.

3. Right click DIVA View 6, 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.

telestream

Configuring the Proxy Storage Location

The Storage Location configuration is located in Administration > Proxy Management > Proxy Storage Locations screen.
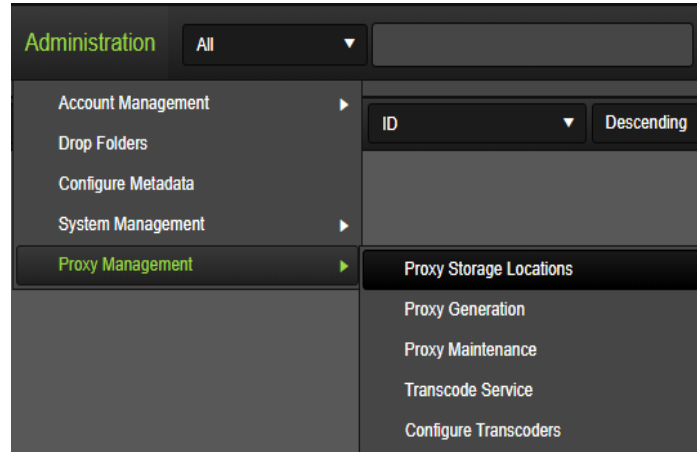
Add a new Storage Location with the same physical and virtual path created in IIS in the previous steps using the following procedure:

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

---

1. Click the Add on the top right side of the screen.

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 DIVAView proxies) in the Virtual Path field.

4. Select the Is Enabled? check box to enable use of the proxy; otherwise leave it deselected.

5. Select either Percent or Bytes from the Limit Type pull down list.

6. Enter a value in the Limit Value text box.

7. Click Insert 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 Watch Folder

Proxy Watch Folders are generally for legacy compatibility. The proxy generation configuration is the preferred method of proxy creation because it is highly configurable and can be managed within the application. PDF files are useful for proxies that are generated outside the DIVA ecosystem, or when upgrading from older versions, where you would like to retain the use of SPM to generate proxies.

You must configure a new Proxy Watch Folder in the Administration > Dropfolders section after you have created the virtual directory in IIS, and configured the Storage Location. See *Watch Folder Configuration* for instructions on creating a Proxy Watch Folder.

Proxy Generation
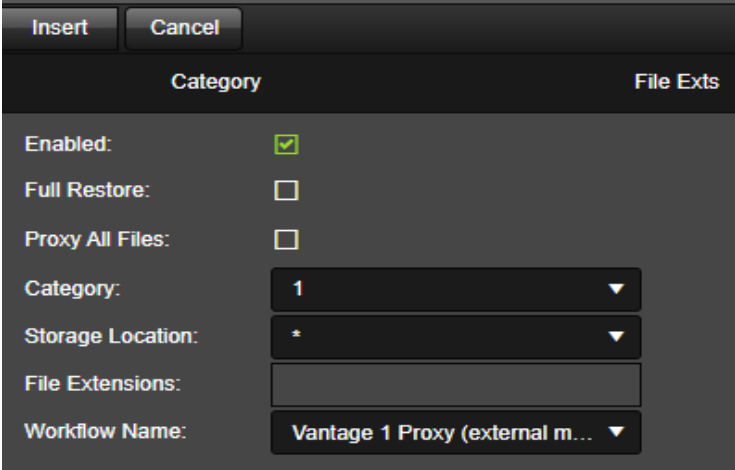
Proxy generation is configured in the Administration > Proxy Generation menu. This section is only available to users in groups that have the Proxy Upload and Generation permissions.
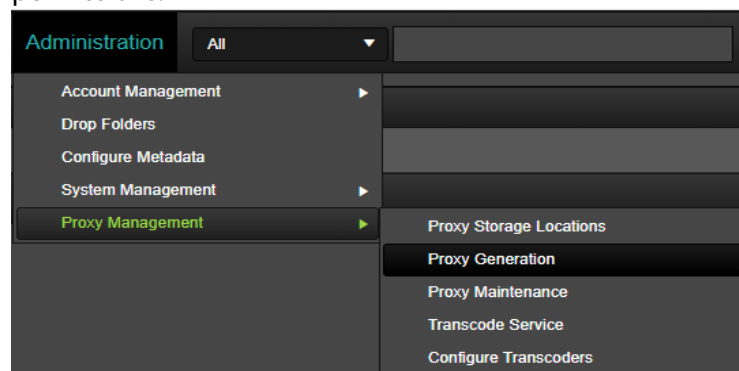
Adding Collection Filters

You can add Collection filters to control which object collections 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 Collection filter:

1. Click Show Configuration tab on the Proxy Generation screen.

2. Click + in the Category Filters section. The following screen is displayed:

3. Select the Is Enabled check box to enable this filter; otherwise leave it deselected.

4. Select the Full Restore check box to enable full restore capabilities; otherwise leave it deselected.

5. Select the Proxy All Files check box to generate a proxy for each file matching the File Extensions filter.

Note: There is a limit of 100 proxies per object. If this check box is left deselected, then only one matching the File Extensions will be selected for proxy creation.

---

6. Select the Collection that should have proxies created for it from the pull down list. You can select the same collection multiple times, but you must differentiate the file extensions in Step 8. You can select the asterisk (*) if the filter should apply to all collections.

7. 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.

8. Enter the file extensions that should have proxies created for them in the File Extensions text box. This is a comma separated list of file extensions (for example, mxf, mov, mp4, and so on).

9. Select the transcoder workflow to use for proxy generation from the Workflow Name pull down list.

10. Click Insert to save the filter.

DIVA Core Restore Options

Next, the DIVA Core options used must be configured to restore the source file. These restore options will also be used for manual proxy generation tasks. Configure the following parameters in the DIVA Core Restore Options section of the screen.

- Queue Size

  Enter the desired Queue Size in the text box, or use the up and down arrows to identify the desired size.

- Map Restore Path

  Select the check box to map the Restore Path; otherwise leave it deselected.

- Remote Path

  Enter the Remote Path in the text box.

- Local Path

  Enter the Local Path in the text box.

- Cleanup Interval

  Enter the Cleanup Interval (in minutes) in the text box, or use the up and down arrows to identify the desired cleanup time.

- Prioritize By

  Use the pull down list to select the desired prioritization (for example, Largest File First, Newest Asset First, Newest Asset First + Until Archive Date, and so on).

- Restore Destination

  Select the Restore Destination Server from the pull down list.

- Root File Path

  Enter the Root File Path in the text box.

- Quality Of Service

  Select the Quality of Service from the pull down list.

- Priority

  Select the Request Priority from the pull down list.

- Options

  Select the desired Options from the pull down list as follows:

  – Default

    The default includes no other options.

  – Prevent File Overwrites

    This option prevents overwriting existing files on the Destination Server.

  – Delete Files Prior to Restore

    This option deletes files with the same filename on the Destination Server before performing the restore.

  – Prevent File Existence Check

    This option will prevent the system from checking and detecting existing files with the same name on the Destination Server as the files being restored.

Scheduling

You can configure proxy generation to run continuously, or only within a specified period. You configure these settings in the Schedule section of the screen. 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.

Schedule			
Enabled	Day	Start Time	End Time
☑	Sunday	12:00 AM	11:59 PM
☑	Monday	12:00 AM	11:59 PM
☑	Tuesday	12:00 AM	11:59 PM
☑	Wednesday	12:00 AM	11:59 PM

Click Save Settings at the top of the page when configuration is complete. Click Start Generation on the top right of the screen to start the generation task. This is a toggle button and will display Stop Generation when clicked. Click the button again to stop proxy generation.

Note: A Status icon has been added to identify if Proxy Generation configuration is within a configured scheduled time. Green indicates it is within a configured scheduled time. Red indicates it is not within a configured scheduled time.

Proxy Generation Preview

After creating the desired filters for Proxy Generation, you can preview the output as follows:

1. Click Preview Generation on the top right of the screen.

2. The following dialog is displayed:
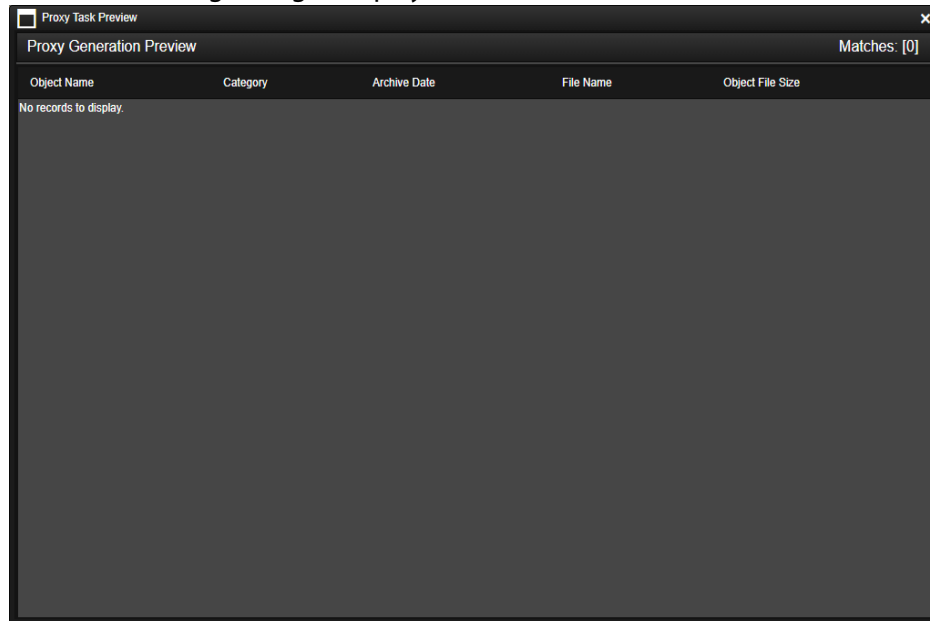
3. After confirming that the preview is what you desire, click the X icon on the top right to close the dialog.

Proxy Maintenance

Proxy Maintenance is configured in the Administration > Proxy Maintenance menu.
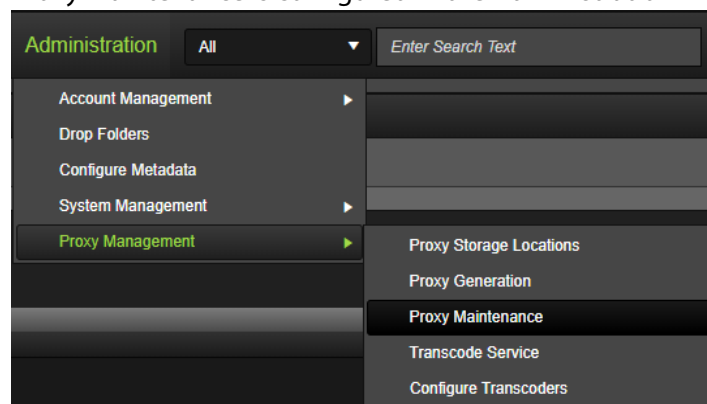
Use the following procedure to configure Proxy Maintenance:

1. Click Show Configuration on the top of the Proxy Maintenance screen. The

following screen is displayed (this is a partial screen shot):

Enable Task:	☐	Object Name:	*
Queue Size:	25 Proxies ▲▼	Object Category:	* ▼
Action:	☐ Proxy ☐ Metadata ☐ Thumbnails	File Name:	*
Workflow Name:	Vantage 1 Proxy (external m... ▼	Proxy Types:	☐ Undefined ☐ MP4
Storage Location:	* ▼		☐ WMA ☐ WAV
Prioritize By:	Largest File First ▼		☐ WMV ☐ MP3
Delete Source File:	☐		☐ MOV
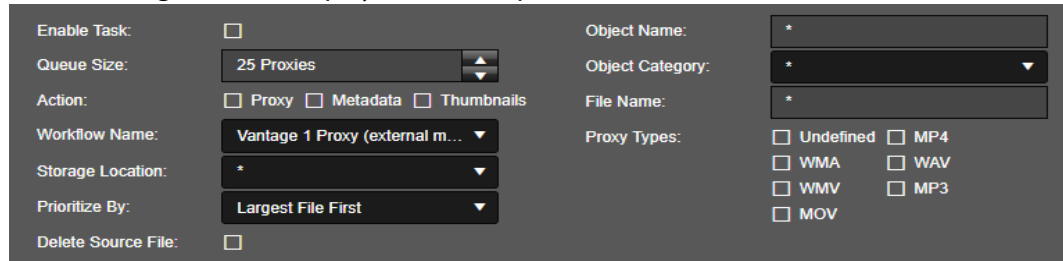
2. Select Remux from the pull down menu on the top left to configure proxy regeneration as shown in the previous figure.

3. Configure the Proxy Remux as desired and click Save on the top right of the screen.

Notes: When selecting the Delete Source File check box, the system will delete the proxy it is remuxing from.

The Proxy Type is a filter for which proxies need to be remuxed. Use the check boxes to select the Proxy Types to be remuxed.

4. Select Purge from the pull down menu on the top left to configure proxy purging as shown in the following figure.

Proxy Maintenance Purge ▼

Enable Task:	☐	Object Name:	*
Action:	Leave Most Recent ▼	Object Category:	* ▼
Backup Files:	☐	File Name:	*
Backup Path:		Proxy Types:	☐ Undefined ☐ MP4
			☐ WMA ☐ WAV
			☐ WMV ☐ MP3
			☐ MOV
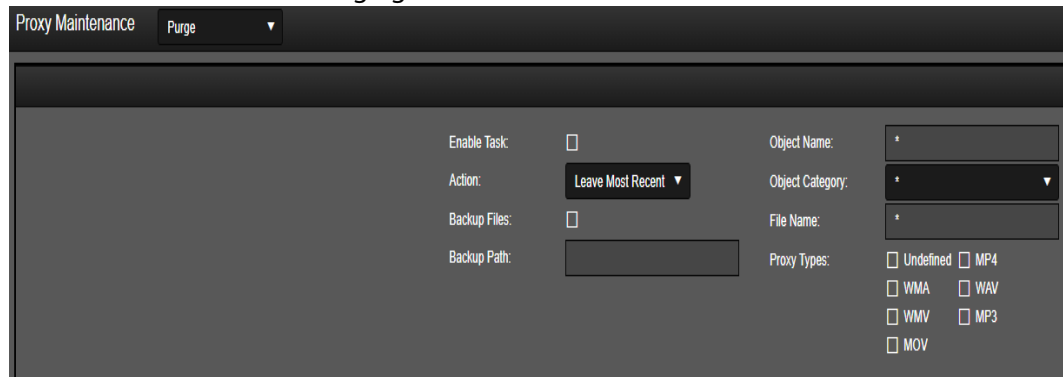
5. Select Audio Extraction from the pull down menu on the top left to configure audio extraction as shown in the following figure.

Audio tracks are auto-generated. In the Player screen the Audio Track selection pull down menu is located to the left of the timecode.

Proxy Maintenance Audio Extraction ▼

Enable Task:	☑	Object Name:	
Queue Size:	5 Proxies ▲▼	Object Category:	* ▼
Use Local Extraction:	☑	File Name:	
Prioritize By:	Newest Asset First ▼	Proxy Types:	☑ MP4 ☐ WMV
			☐ MOV
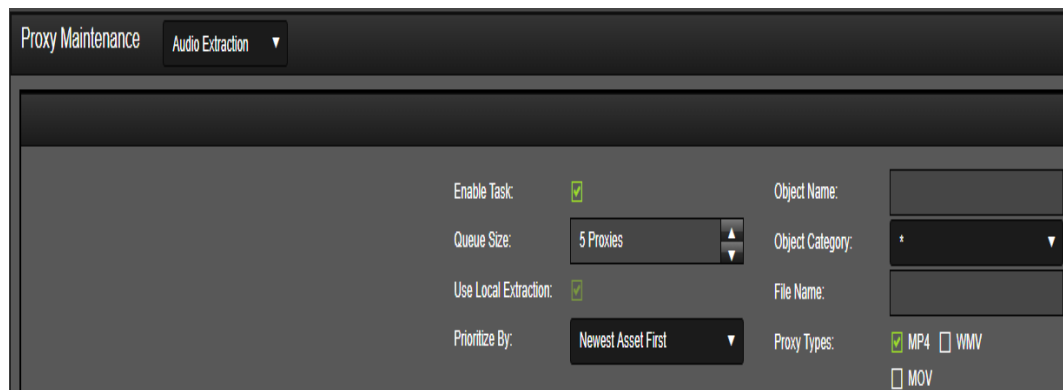
6. Proxy maintenance can be configured to run continuously, or only within a specified period. You configure these settings in the Schedule section of the screen. A list of check boxes and time selectors are displayed next to each day of the week.

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.

telestream

Transcode Service Configuration

Before configuring the transcoders you must confirm that the Windows Service is running. Open Windows Services and confirm the status of the Telestream.Transcode.Host service. If it is not running then you must start it by right clicking the service name and selecting Start from the context menu.

You configure the Transcode service through the DIVA View web interface. Navigate to the Administration > Configure Transcoders. 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 are set correctly.

Note: FFmpeg and Vantage are supported for use with the transcode service. Other transcoders can be integrated using custom scripts that are provided by Telestream as an additional purchased service from the Professional Services Group.

Use the following procedure to configure the transcoder settings:

1. Set the transcoder URL in the URL text box.

   The status of the transcoder is displayed in the Status text box and the transcoder version number is displayed in the Version text box (these two fields are uneditable).

2. Under the Local Transcode Operations section:

   – Enable Local Transcode Operations

   Select the check box to enable transcode operations locally; leave it deselected to disable this option. This options requires a path to the FFMpeg instance on the local service, but it optimizes the extraction for these so they do not have to be passed to a separate service and queued.

   – Path To Transcode Executables

   Enter the path to the transcoder executables in the text box.

   – Enable Local Audio Extraction

   Select the check box to enable transcode operations locally; leave it deselected to disable this option.

   – Enable Local Frame Extraction

   Select the check box to enable transcode operations locally; leave it deselected to disable this option.

3. Under the Locations section click Add to add a new location. The following screen is displayed:

4. Enter the location name in the Name text box.

5. Enter the path to the transcoder in the Path text box.

6. Select the Is Default check box if this transcoder is going to be the default.

7. Click Insert to add the location.

telestream

Starting and Stopping the Transcode Service Windows Services

The Windows service installed with the Transcode Service should be set to start automatically. The service displays in the Windows Service Manager using the name Telestream.Transcode.Host.

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

- 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 and Background Task Service:

```
Telestream.Transcode.Host start
```

Configuration File Changes

The DIVAView.TaskManager Windows Service configuration file (DIVAView.TaskManager.exe.config) is located in the C:\Program Files (x86)\DIVAView 6\TaskManager\ folder.

The configuration file has four main sections that need your attention as described in the following procedures:

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="DIVAView"/>
     ```
   – 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" />
     ```
   – DIVACoreApiUrl

     This parameter identifies the WS API REST endpoint.

     ```
     <add key="DIVACoreApiUrl" value=" https://DIVA-VM-105:9444/
     diva/service/rest/2.2/DIVACoreWS_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="kAkWTK3ObnEOmHheJAKP" />
     ```
   – DWSVersion

     This parameter is the version of the API service that DIVA View 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 register-Client 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" />
```

– DIVACoreApiUrl

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

```
<add key="DIVACoreApiUrl" value="http://10.80.106.57:9763/
services/DIVACoreWS_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 DIVA View. 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 DIVA Core Restore request (through the DIVA Core Web Services API REST endpoint), and initiates a Transcode request upon completion. This task is also responsible for calling the Proxy Creation Service.

– DIVACoreSyncTask

This task controls synchronizing objects with DIVA Core.

telestream

– UpdateRequestsStatusTask

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

– CreateProxyOnRequestCompleteTask

This task is responsible for creating proxies in DIVA View by sending requests to the transcoding service when a DIVA Core 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 DIVA View for transcode Requests not associated with a DIVA Core 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 Standalone 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 DIVA View 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.

telestream

Configuring the Vantage Standalone Presets

Navigate to Administration > Proxy Management > Configure Transcoders
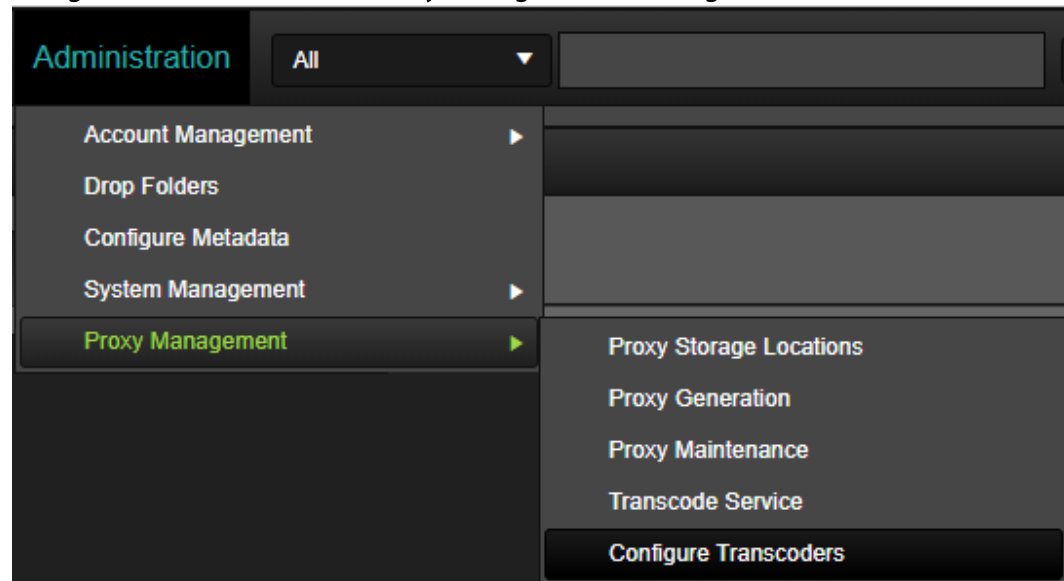
Task 1 Configure Transcoder Settings

1. Click the Red Plus (+) button to create a new transcoder.
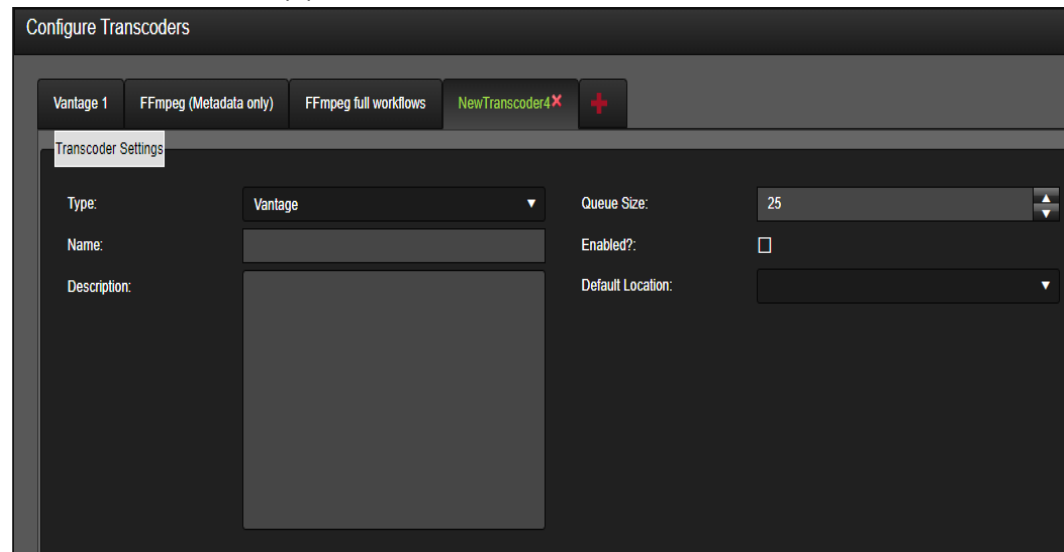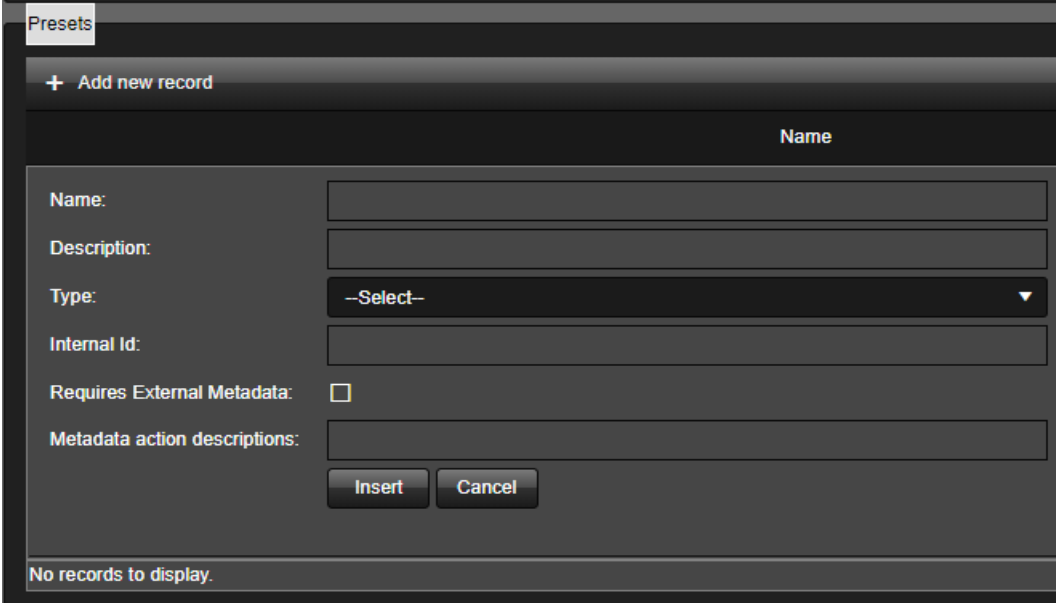
2. In Transcoder Settings, select Vantage for the type.

3. Enter a unique name for the transcoder in the Name text box.

4. Enter additional descriptive text in the Description text area.

5. Adjust Queue Size if needed. This value will determine the number of simultaneous transcode Requests the transcoder can accept.

6. Select the Enabled? check box to activate this transcoder and allow it to be used in DIVA View workflows.

7. Set the server hosting the Vantage SDK service using the pull down list in the Location field.

8. Enter the IP address of the server hosting the Vantage SDK service in the IP Address text box.

9. Enter the port used by the Vantage SDK service in the Port text box. On default installations, this will be port 8676.

Task 2 Define Presets

1. In the Presets panel, click + Add new record. The following screen is displayed:

2. Enter a name for the preset in the Name text box. 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*.

3. Enter a short description for the preset in the Description text box.

4. Use the pull down list to select the preset type:

– Video Proxy

Creates a proxy with automatic or manual workflow.

– Thumbnail Only

Extracts thumbnail images for EDLs (such as Shot List page).

– Metadata Only

Extracts the required metadata fields for proxy generation. This is used for configuring split workflow setups. See *Configuring Vantage Split Workflow*.

– Thumbnail & Metadata

Extracts thumbnail images and metadata for use in Watch Folders configurations.

telestream

5. Set the Internal Id to match the Vantage Workflow Id of the corresponding workflow.

6. If you are using a Video proxy preset in a split workflow configuration (for example, Vantage server without an Analysis license), then select the Requires External Metadata check box. See *Configuring Vantage Split Workflow*.

7. Enter any Metadata Action Descriptions in the text box. 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 the 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.

8. Click Insert, and then Save to save the new Preset.

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 Administration > Proxy Management > Configure 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. Enter a unique name for the transcoder in the Name text box.

4. Add additional descriptive text in the Description text box.

5. Adjust Queue Size if needed. This value will determine the number of simultaneous transcode Requests the transcoder can accept.

6. Select the Enabled? check box to activate this transcoder and allow it to be used in DIVA View workflows.

telestream

Task 2 Define Presets to Produce Required Metadata for Proxy Generation

1. In the Presets panel, click + Add new record.

2. Enter a name for the preset in the Name text box. 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 from the drop down list.

4. Enter the fully qualified path to the executable (without parameters) to be used for extraction in the exe path text box.

In a default setup this path is used:

```
C:\Program Files (x86)\EcoDigital\TranscodeService\Plugins\ffpr
obe.exe
```

5. Enter the arguments to pass to the executable previously entered in the exe arg text box.

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 request.

6. Select the Ignore StdError Output check box if the exe will write output to std error that should not be interpreted as an error; otherwise leave it deselected.

7. Select the Rename Thumbnails? check box if you want to rename the thumbnails associated with the proxy; otherwise leave it deselected.

8. Enter the interval for thumbnails in the Thumbnail Interval In Sec text box.

9. Click Insert, and then Save.

telestream

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

1. On the Vantage server, create 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)\EcoDigital\TranscodeService\SampleWorkf
   lows\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 check box.

   When this option is selected and a Request 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 Request 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 Insert, and then Save.

Multiple Transcoders and Load Balancing

With DIVA View 6.1.0.209, 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 Collection will be distributed between Vantage1 and Vantage2:

1. The preset name does not have to be shared, but it must be the same for both servers.

2. Follow the steps in *Configuring the Vantage Standalone Presets* to configure the Vantage1 server.

3. Create a Video Proxy preset with name shared in Vantage1.

4. Save the Vantage1 configuration.

5. Follow the steps in *Configuring the Vantage Standalone Presets* to configure the Vantage2 server.

6. Create a Video Proxy preset with name shared in Vantage2.

7. Save the Vantage2 configuration.

8. Navigate to Administration > Proxy Management > Proxy Generation.

telestream

9. Create a new Collection Filter with workflow name set to shared.

Command Line Transcoder and 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)\EcoDigital\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 Administration > Proxy Management > Configure 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 in the Name text box.

4. Add additional descriptive text to the Description text area.

5. Adjust the queue size if needed. This value will determine the number of simultaneous transcode Requests the transcoder can accept.

6. Select the Enabled? check box to activate this transcoder and allow it to be used in DIVA View workflows.

7. Select the Parse output for progress? check box to parse the transcoder output.

8. Select the Execute Immediately? check box if you want to execute the transcoding preset immediately.

9. Select the Produces Metadata Only? check box if this transcoder will only produce metadata.

10. Select the Ignore StdError Output check box if the exe will write output to std error that should not be interpreted as an error.

telestream

11. Select the Rename Thumbnails? check box if this transcoder will be allowed to rename thumbnail files.

12. Select the Thumbnail Interval In Sec: enter the number of seconds to delay when creating thumbnails in the text box.

Task 2 Define Custom Command Video Proxy Preset

1. In the Presets panel, click + Add new record button.

2. Enter a name for the preset in the Name text box. 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 from the drop down list.

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 previously entered. In a default setup, this is:

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

6. Select the Ignore StdError Output check box if the exe will write output to std error that should not be interpreted as an error.

7. Click Insert, and then Save.

Custom Script Parameters

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

- {{input_filepath}}

  The fully-qualified path of the input file to the custom script.

- {{output_basepath}}

  The fully-qualified base path for storing the proxy artifacts. This is a temporary sub-directory stored under the staging location. Files output by the transcoder will be stored here until they are transferred by the DIVA View Task Manager service to the proxy storage location.

- {{output_filename}}

  The 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.

telestream

Daily Operations

DIVA View must be monitored daily to insure proper operation, storage capacities, orphaned files, user interaction, successful backups, and general system health. When logged in as a System Administrator the System Status Icon in the lower left corner of the screen displays a snapshot of messages to look for. Click the question mark icon to get a full list of the running state of the application. This includes monitoring storage locations and so on. If you discover any anomalies that you are uncertain of or if you are unsure of how to handle them, contact Technical Support for assistance.

Topics:

- Checking Available Storage Capacity
- Checking for Orphaned Files
- Checking Audit Trails
- Checking for Successful Backup Completion
- Monitoring Proxy Generation

Checking Available Storage Capacity

In your initial DIVA View 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 *Configuring the Proxy Storage Location*) or configure a new location.

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

1. Navigate to the Administration > Proxy Management > Proxy Storage Locations.
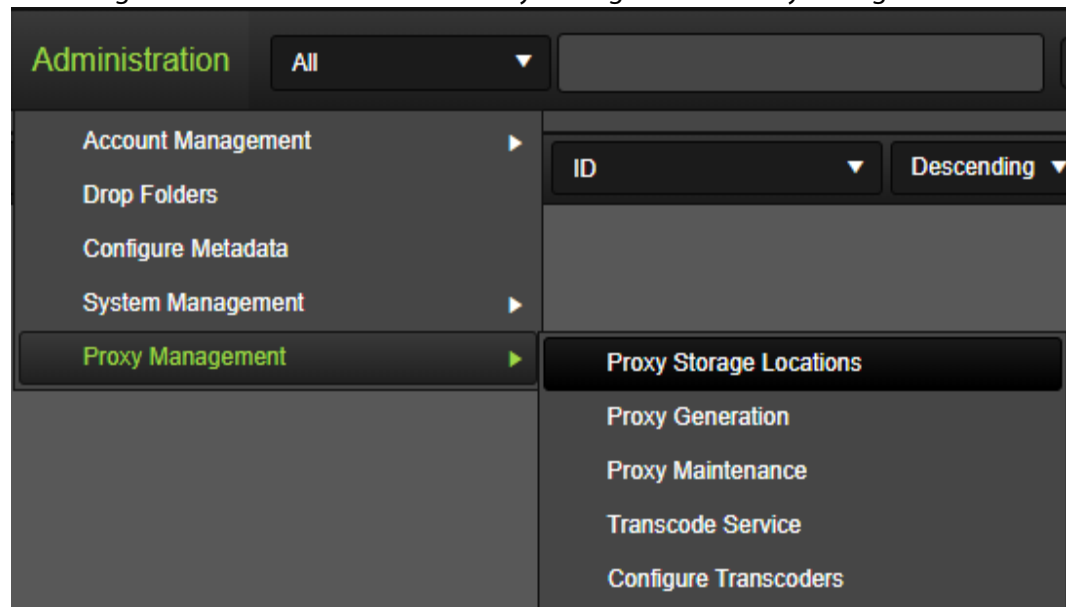
2. Check each location's State to identify the current storage location status.

If the location's state is something other than Online (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 can use the Server logs and Watch Folder logs to help identify issues; see *Logging Configuration* for details on the various log locations. If you are unable to resolve the issue and need further assistance contact Technical Support.

3. Check the Used Space column to identify how much of the storage space is filled and how much is left available 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 the storage space limits must be adjusted, refer to *Configuring the Proxy Storage Location*.

5. If data must be migrated to another storage location, refer to *Configuring the Proxy Storage Location* for information.

Check for orphaned files next.

Checking for Orphaned Files

Throughout daily user interaction with DIVA View, you will occasionally get some orphaned files. Orphaned files are files that were placed in a Watch Folder and had the wrong format, had different encapsulation than configured for the folder, or referenced an object that does not exist in the DIVA View database (other than Virtual Objects). 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 *Watch Folder Configuration*).

Note: There can be Orphan files for the Metadata Watch Folder, the Proxy Watch Folder, and the Annotations Watch Folder.

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 Watch 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 Watch 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.

Check the user interaction with audit trails next.

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.

Navigate to the Administration > System Management > Audit Trail menu item.
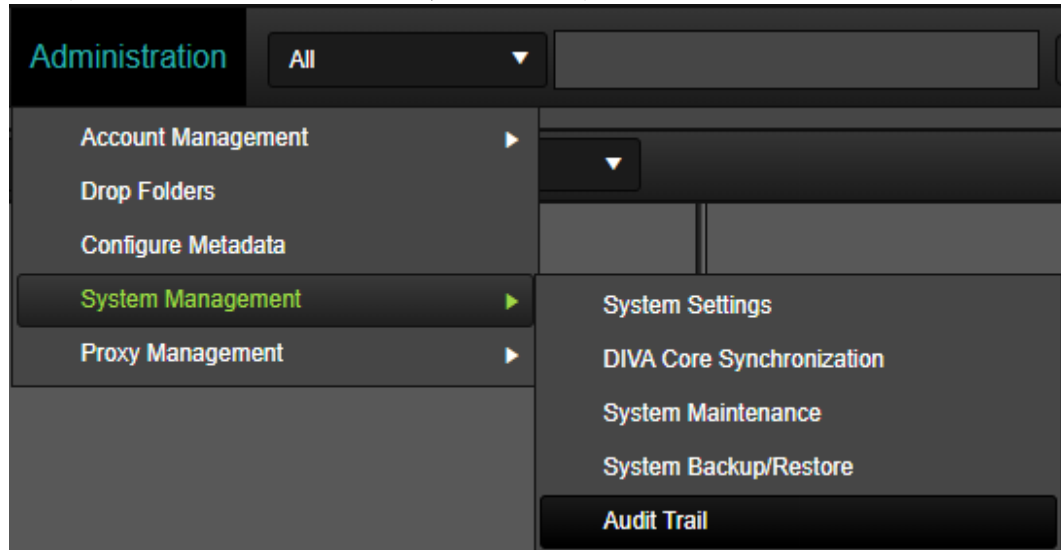
The Audit Trail screen displays user interactions with the DIVA View system.

You can filter the display by Action, Organization, Group, User, Time (From and To), Object Name, and Object Collection. Click the Show Filters button to access the filters. using the options on the right side of the screen. The Object Name and Object Collection 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 Collection MOV:

1. Select the Organization check box, and then use the pull down list to select Marketing in the Organization field.

2. Select the Object Name check box, and then enter My in the Object Name text box.

3. Select the Object Collection check box, and then enter *MO* in the Object Collection text box.

4. Press Enter to apply the filter.

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

   You can order the results using the Order By: pull down list at the top of the Audit Trail screen.

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 into either a CSV or XML file.

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 DIVA View Database Backup 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 Request. 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.

Notes: Under normal operations where new objects are archived daily, it is expected that the Database Backup size increases over time.

DIVA View does not remote copy secure daily database backups (for example, copy each newly created backup to another server). Securing this data is the customer's responsibility.

Monitoring Proxy Generation

The administrator should monitor the Proxy Generation at least once every 24 hours to confirm that they are being created, or purged, on schedule.

Select the Administration > Proxy Management > Proxy Maintenance menu item to view the Proxy Maintenance screen. The screen opens with the Monitor tab selected and displays the Generation History. The following figure is a compressed screenshot.

You can search the generation history using specific filters or view all history in the Generation History area of the screen. At the top of the Generation History section of the screen is a quick-view bar showing the number of proxies Completed, currently Restoring, currently In Progress, Failed and Cancelled.

Clicking on the Show Configuration button on the top right will display the Proxy Generation Configuration (this is not the same as the Proxy Generation screen - this screen is for maintenance). On the Configuration screen you can Regenerate Proxies that have failed, manually Purge Proxies, and Schedule proxy generation. Click on the name of the title bar you want to expand to view the options available.

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 DIVA View. 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.

Topics:

- Database Synchronization Management
- Proxy Storage Management
- User Data and Resource Management
- Search Management
- Session Management

telestream

Database Synchronization Management

You added database synchronization filters in your initial DIVA View 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. Navigate to Administration > System Management > DIVA Core Synchronization menu item.
2. Click the Show Scheduling button on the top right side of the screen.
3. Select the filter to edit and click the Pencil icon to enter the Edit screen
4. You can now make any necessary changes to the filter.
5. Click the green Check Mark icon to save your changes; otherwise click the red X icon to cancel editing.

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

1. Navigate to Administration > System Management > DIVA Core Synchronization menu item.
2. Select the filter to edit and click the Pencil icon to enter the Edit screen.
3. Either select the Enable check box to enable the filter or deselect the check box to disable the filter.
4. Click the green Check Mark icon to save your changes; otherwise click the red X icon to cancel editing.

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

1. Navigate to Administration > System Management > DIVA Core Synchronization menu item.
2. Locate the filter you want to remove in the list.
3. Click the red X icon on the right side of the filter entry.
4. 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 DIVAdirector 5.3 and below. To find the migration progress and a check box to enable the storage migration, go to Administration > Proxy Management > Proxy Storage Locations. These are only visible if there are eligible proxies to migrate.

User Data and Resource Management

Users have the ability to share their private data so other users can see it including Queries, Work Bins and Shot Lists. After a user shares a resource they can unshare it using the Sharing pull down list on each of the mentioned pages (that is, Queries, Work Bins, or Shot Lists respectively).

Unsharing a Public Resource

Caution: If you select the Not Shared menu item, the selected resources become private without additional confirmation.

You manage public resources such as Queries, Work Bins and Shot Lists on   each specific screen (that is Queries, Work Bins, or Shot Lists screens respectively). Any item shared by a user can only be unshared again by the user from each respective page.

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 and Management*.

Note: Deleting Organizations, Groups or Users will only be soft deletes (they are not removed from the database) so that the audit trail retains references to deleted entities. This also allows for easy restoration of deleted entities, so that reconfiguration does not need to occur for something that was deleted by mistake.

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 or Editing 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.

telestream

1. Navigate to the Administration > Account Management > Configure Organization 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 Administration > Account Management > Configure Organization 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 or Editing a Group* for instructions on adding groups.

Modifying an Existing Group

Use the following procedure to modify an existing group:

1. Navigate to the Administration > Account Management > Configure Group 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 on the Permissions tab, metadata permissions in the Permissions (Metadata) tab, the DIVA Core settings in the DIVA Core Settings tab, and the group export settings on the Export Settings tab. Content filters are discussed in the *Content Filter* section.

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.

telestream

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

1. Navigate to the Administration > Account Management > Configure Group screen.

2. Select the group name to delete from the Group pull down 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 or Editing 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 Administration > Account Management > Configure 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 Technical Support for assistance. The last user in the SystemAdmins group can never be deleted.

1. Navigate to the Administration > Account Management > Configure 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.

4. Click OK in the confirmation dialog box to delete the entry.

telestream

Search Management

You can add, update, or delete metadata at any time. You added metadata, defined content filters, and assigned metadata publishing roles during the initial system configuration. All modification and deletion of metadata entries occur on the Administration > Configure Metadata screen. See *Metadata Configuration* for instructions on adding search metadata.

Metadata Column Manager

The Administration > Configure 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.

Metadata Columns can be added, removed, edited, and reordered for on-screen display in the Metadata Column Manager table. Certain rows, such as the parameters from DIVA Core and Proxy Metadata, are predefined, will be always present in the table, and cannot be deleted.

The order of the entries can be changed by dragging and dropping the row to another position to complete the repositioning.

Select the Hidden check box to hide the entry from the Metadata screen; otherwise leave it deselected so it displays on the screen.

Editing a Metadata Entry

Use the following procedure to edit a Metadata Column:

1. Navigate to the Administration > Configure Metadata screen.
2. Locate the metadata entry to edit.
3. Click the Pencil icon in the first table column of the entry row.
4. The selected row is highlighted in the table and all parameters of the selected entry are displayed for editing.
5. When you are finished editing the entry, click the green Check Mark icon to save the changes or click the red X icon to cancel the changes.

Deleting a Metadata Entry

Use the following procedure to delete a metadata entry:

1. Navigate to the Administration > Configure 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.

telestream

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 Administration > Account Management > Manage Sessions screen.

   Online users are displayed in the middle 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.

To log the user off from the system, click the user's name (anywhere on the row) and then right-click an online user and then select Sign out user from the context menu.

Troubleshooting and Disaster Recovery

This chapter includes information for preliminary system troubleshooting and disaster recovery. You should perform these activities before contacting Technical Support for assistance.

Topics:

■ Troubleshooting Tools

■ Task Manager and DIVA View API Windows Services

■ Starting and Stopping the DIVA View Web Server

■ Checking Log Files

■ Manual Database Backup

telestream

Troubleshooting Tools

Telestream recommends that our customers add and install several 3rd party tools that help troubleshooting for their own DIVA View Administrators but also for DIVA View Support when they connect to the server. Technical Support recommends the following tools:

- Log File Viewing and Editing

  https://www.log4view.com/

  https://notepad-plus-plus.org/

- Deeper Web Traffic Analysis (this is more for DIVA Support and DIVA lab)

  https://www.telerik.com/fiddler

  https://www.wireshark.org/

Task Manager and DIVA View API Windows Services

The DIVA View installer will install two additional Windows services and the DIVA View web application. Both of these services can be configured 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 DIVA View. The binaries for this service are installed in the TaskManager subdirectory, located under the DIVA View installation directory (for example, C:\Program Files (x86)\DIVAView 6\TaskManager). This service is visible in the Windows Services console under the name Oracle.DIVAView.TaskManager.

telestream

DIVA View API Service

The DIVA View 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.

Note: Technical Support recommends using archiving tools such as FTP Server, SFTP Server, cloud-based file transfer and file management tools for Local Archives that include files greater than 2 GB.

The binaries for this service are installed in the Api subdirectory located under the DIVA View installation directory (for example, C:\Program Files (x86)\DIVAView 6\Api). This service is visible in the Windows Services console under the name Oracle.DIVAView.Api.

Starting and Stopping the DIVA View Web Server

You can start and stop the DIVA View 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 DIVA View 6 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

DIVA View creates log files for both the system and for Watch Folders during normal operations. You configured the log file names, sizes and locations in the initial DIVA View configuration. See *Logging Configuration* if you need a reminder of the file names and locations you assigned to the logs.

The DIVA View server logs contain information regarding the various server operations and possible operation processing error information. The Watch Folder logs contain information specific to the Watch Folders.

Logs are also sent to UDP port 7071 so they can be aggregated in a log view, for example Log4View. This allows troubleshooting the interactions of multiple services simultaneously because they all report to this port.

You can find the web server logs in the %DIVAView_HOME%\www\logs\log.txt file. The web server logs are used for troubleshooting the system and may be requested by Technical 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 DIVA View server logs set the log level no higher than Level 2 unless trying to locate an error or instructed to do so by Technical Support.
- For Watch Folder logs set the log level no higher than Level 0 unless trying to locate an error or instructed to do so by Technical Support.

Manual Database Backup

The manual backup of the database is a very important operation in any data system. DIVA View provides you a simple way to perform this operation when necessary.

Performing a Manual Backup

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

1. Navigate to the Administration > System Management > System Backup screen.

telestream
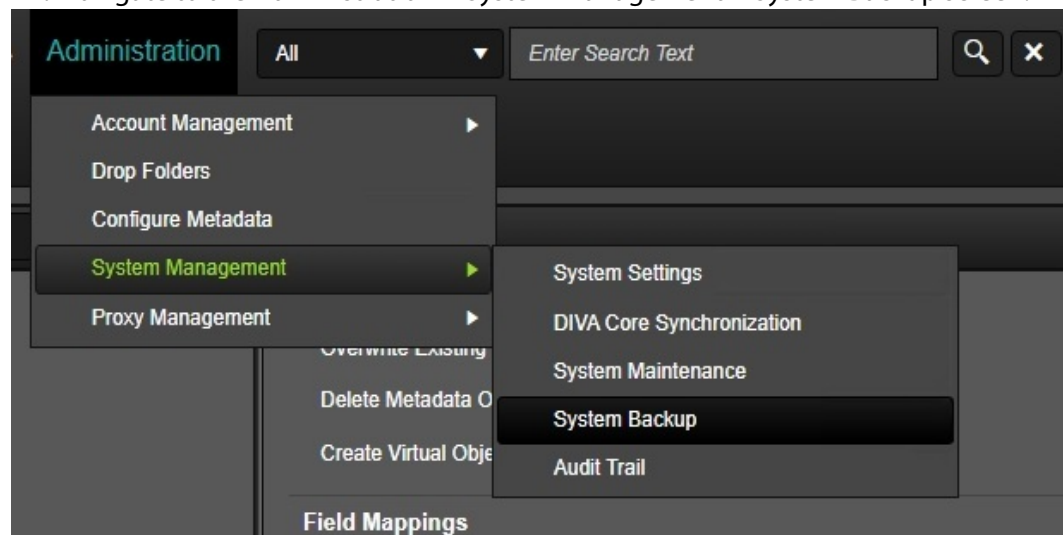
2. At the bottom of the screen is a list of previous backups. Click the Manual Backup icon at the top of this section.

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

The timestamp format is YYYYMMDD-hhmm, where:

– YYYY = year

– MM = month

– DD = day of month

– hh = hour

– mm = minute

3. When the confirmation dialog box appears, click OK to confirm you want to perform a manual backup; otherwise click Cancel to terminate the operation.
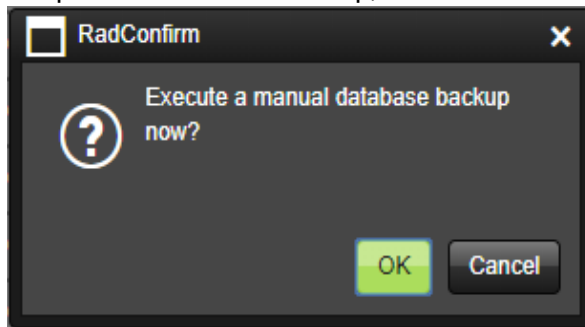
A dialog box will appear stating that the backup process has started and normally takes approximately 3-5 minutes to complete (depending on the amount of data in the database).

Frequently Asked Questions

- Why Does DIVA View Require a License File?

  Telestream has re-introduced license file checking starting with DIVA View 6.0. If you do not have a valid License, please contact your Sales Representative.

- Do Proxy Watch Folders exist and are they still usable?

  Yes, they still exist in this release and can be used. Telestream recommends using the Transcode Service rather than Proxy Watch Folders for associating proxies with objects in DIVA View.

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

  Yes, the original proxy workflow still exists and is usable in this release. Proxies are created without control and outside of DIVA View. Then they are sent to DIVA View using the Proxy Watch Folders.

- What releases of DIVA Core does DIVA View support?

  DIVA View 6.1.0.209 supports DIVA Core 7.4 and later.

- Can DIVA View 6.1.0.209 list all component files of a DIVA Core Complex Object?

  Yes, DIVA View can list all Complex Object component files.

- Can DIVA View 6.1.0.209 restore any component file of a DIVA Core Complex Object?

  Complex Object support is currently implemented in releases 5.4 and later.

- 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 DIVA Core and DIVA View. However, the Local Proxies feature still works in this release.

- Do Watch Folders support DIVA Core Partial File Restore?

  DIVA Core Operation Watch Folders support Partial File Restore operations.

telestream

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

  The transcoder will proxy a source file with valid file extensions when a request is made to the Transcoder Server from DIVA View. 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 is supported through its API interfaces. FFMpeg is custom integrated into DIVA View given that its command line interface will provide DIVA View with the frames and metadata required.

  Additional transcoders could be supported but will be restricted in that the command line interfaces can be accessed through custom scripts. See *Transcode Service Configuration* for detailed information.

telestream

Additional Configuration Information

Topics:

telestream

Adding Proxy Storage

This section describes how to add a Proxy Storage Location. Use the following procedures to add a new Proxy Storage Location.

Proxy Storage Structure Changes During Upgrades

DIVA View 6.1.0.209 will perform a directory structure change on proxy storage locations when upgrading from DIVAdirector 5.3 or prior. To revert this change in case of rollback, a script will need to be generated from the original database export. Take this into account when creating an upgrade plan from earlier versions, and contact Technical Support to obtain the corresponding script.

When upgrading from DIVAdirector 5.x to DIVA View 6.x there are changes to the proxy storage structure, and frames extraction. In earlier DIVAdirector releases (5.x) Proxies were stored in a range of subfolders numbered 0 through 100 on the configured storage location. Each related database entry and the full path to the proxy was located in the proxies database table.

The proxy directory structure change was implemented in the DIVAdirector 5.3 release. The design change included the following:

- One subdirectory per object (<Proxy Storage Directory>/(Object base_id)/)
- One subdirectory for Asset Images (<Proxy Storage Directory>/(Object base_id)/AssetImages/<object asset images>)
- One subdirectory for Binary File Uploads that is created when the file is uploaded (<Proxy Storage Directory>/(Object base_id)/BinaryFiles/<object binary meta-data>)
- One subdirectory per Proxy (<Proxy Storage Directory>/(Object base_id)/<proxy_id>/)
- One subdirectory for Keyframe storage (<Proxy Storage Directory/<Object base id>/<proxy_id>/Keyframes/<proxy keyframe(s)>)

This new layout breaks the previous DIVAdirector 5.2 Proxy Storage Structure. When the database has paths that are not in the new format, a check box and status bar are visible on this page to begin the storage migration. This is a very important step in upgrades because users will not be able to playback proxies without this process finishing. Contact Technical Support for assistance migrating to the new structure or to Enable Legacy Storage Migration if necessary.

telestream

Set IIS Web Server Permissions

1. First map the location so that it is visible in Windows Explorer. An UNC location must be mapped to a drive letter and folder first. If the location is a networked drive, make sure it is set to auto-connect on Windows startup. In Windows Explorer, right click the folder and select Properties.
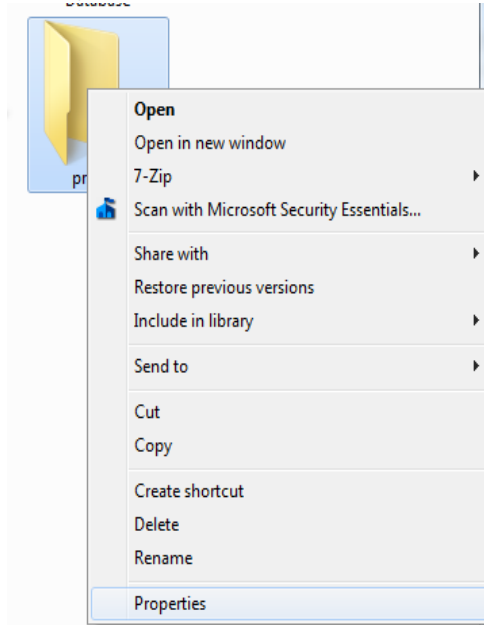
2. On the Security tab click Edit.
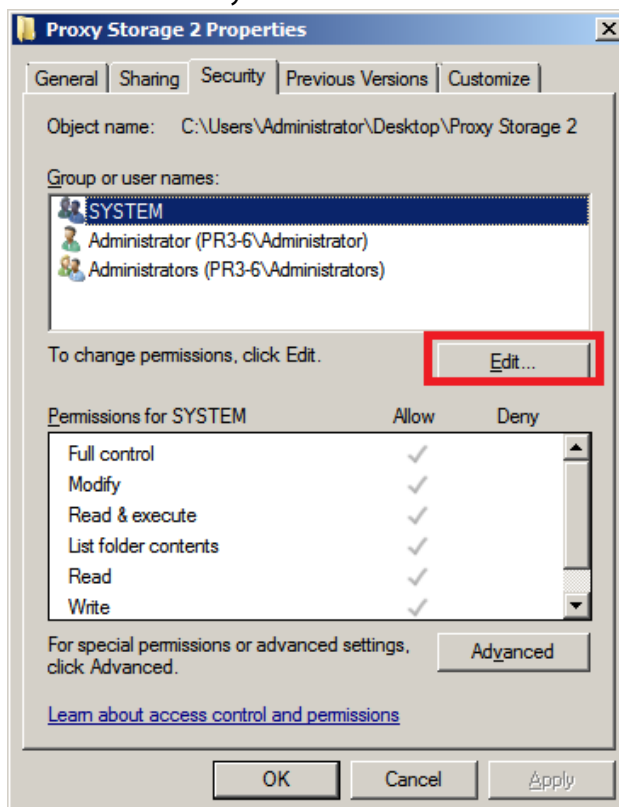
3. Click Add.
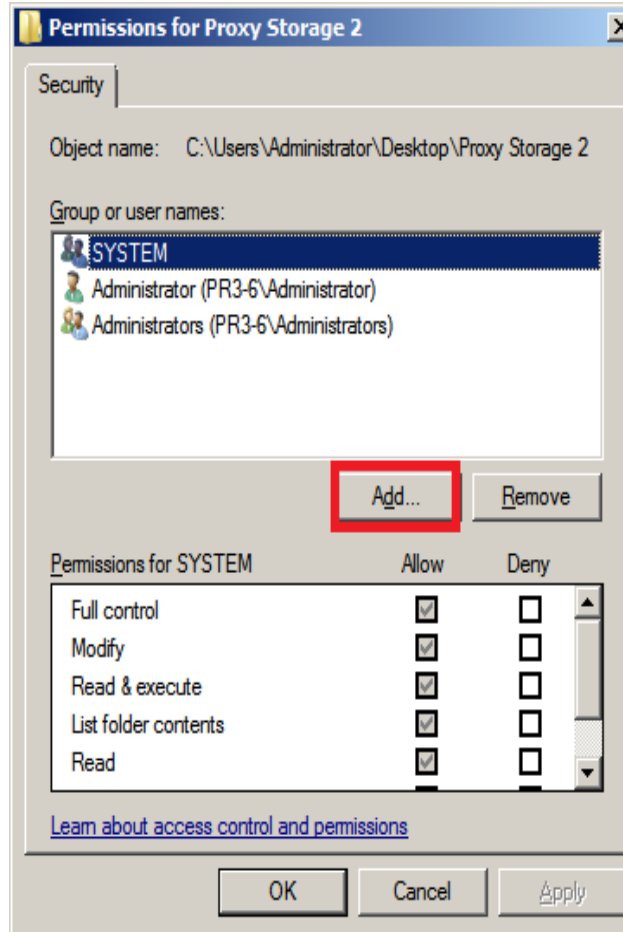
4. Input the IIS Web Server account (default is dd6-user) used during installation in the Object Name text area and click Check Names.
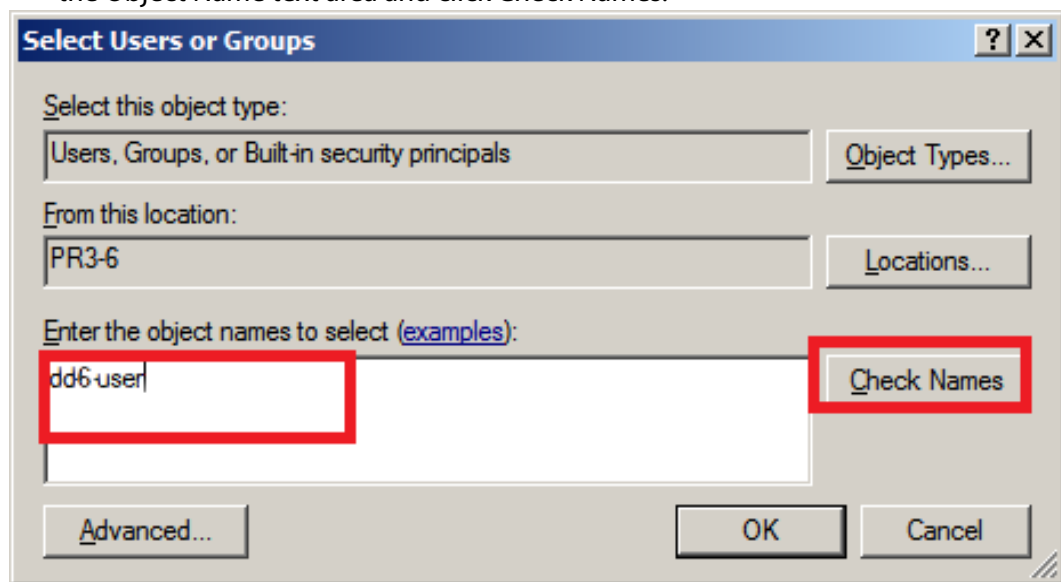
5. Click OK.

6. Repeat the previous steps for Authenticated Users.
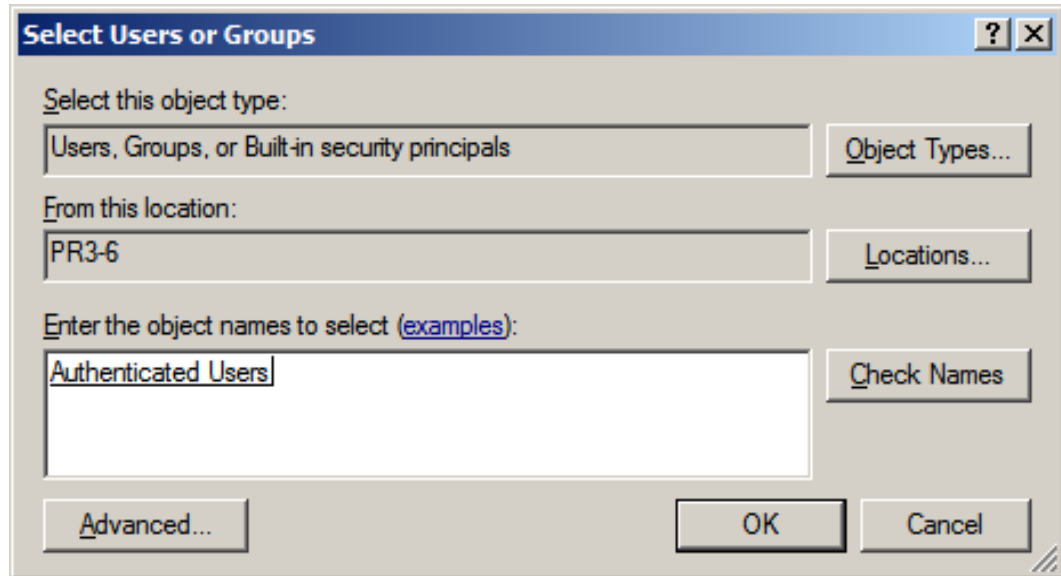
7. The permissions are now set correctly for the DIVA View Web Server.

Adding the Proxy to the IIS Folder

1. Click Start in Windows and type *inetmgr* in search box, then press Enter.

2. In inetmgr click <server-name> (typically DD6SERVER) > Sites > DIVA View 6.

3. Right-click DIVA View 6 and select Add Virtual Directory... from the context menu.

4. Enter an alias name and input the physical path of the new proxy storage location, and then click OK to finish.

telestream

Watch Folder Configuration Samples

Annotation Watch Folder Configuration and Log Files

The following is a sample of the configuration file to drop into the Annotation Watch Folder (see *Additional Annotation Watch Folder Configuration*).

Caution: Do not enter empty lines with the carriage returns; this will cause an error.

```
Object Name,Category Name,Object Identifier,Start Time Code,End
Time Code,Description
"lFv0GB9l2kx2msVYTNaK","FFmpeg2","","00:00:02.02","00:00:03.12","A
nnotation 1: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK"
"lFv0GB9l2kx2msVYTNaK","FFmpeg2","","00:00:05.02","00:00:08.12","A
nnotation 2: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK"
"lFv0GB9l2kx2msVYTNaK","FFmpeg2","","00:00:05.02","00:00:09.22","A
nnotation 3: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK"
"lFv0GB9l2kx2msVYTNaK","FFmpeg2","","00:00:06.02","00:00:10.12","A
nnotation 4: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK"
```

The following is a sample of the log file for the Annotation Watch Folder when viewed in the DIVA View TaskManager (see *Additional Annotation Watch Folder Configuration*).

```
04-21 12:42:08.115 INFO 41
Telestream.DIVAdirector.TaskManager.Dropfolders.DropFolderProcessT
ask - Processing file: [S:\DV\DROP FOLDERS\ANNOTATION_DF\DIVA-
937_annotation_DF_sample_file.txt].
04-21 12:42:08.222 INFO 41
Telestream.DIVAdirector.TaskManager.Dropfolders.DropFolderProcessT
ask - File: [S:\DV\DROP FOLDERS\ANNOTATION_DF\DIVA-
937_annotation_DF_sample_file.txt] processed successfully.
```

The following is a sample of the corresponding Log File for the Annotation Watch Folder in the S:\DV\Drop Folders\Annotation_DF\Log as configured in the *Additional Annotation Watch Folder Configuration* section.

```
Row #: [1] Parsing Started.
Creating EDL entry for Object name, category, file:
[lFv0GB9l2kx2msVYTNaK/FFmpeg2/] with values: [00:00:02:02/
00:00:03:12/Annotation 1: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK].Row #: [1] Parsing Complete.
Row #: [2] Parsing Started.
Creating EDL entry for Object name, category, file:
[lFv0GB9l2kx2msVYTNaK/FFmpeg2/] with values: [00:00:05:02/
00:00:08:12/Annotation 2: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK].Row #: [2] Parsing Complete.
Row #: [3] Parsing Started.
Creating EDL entry for Object name, category, file:
[lFv0GB9l2kx2msVYTNaK/FFmpeg2/] with values: [00:00:05:02/
```

telestream

```
00:00:09:22/Annotation 3: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK].Row #: [3] Parsing Complete.
Row #: [4] Parsing Started.
Creating EDL entry for Object name, category, file:
[lFv0GB9l2kx2msVYTNaK/FFmpeg2/] with values: [00:00:06:02/
00:00:10:12/Annotation 4: test to add an annotation for OBJECT
LFV0GB9L2KX2MSVYTNAK].Row #: [4] Parsing Complete.
Elapsed Time: 127ms
```

Proxy Watch Folder Formatting

DIVA View 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 DIVA View 6.0. To support this functionality, proxies dropped into a Proxy Watch 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, Collection, 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 Collection 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 DIVA View.

- 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, Collection, 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.

telestream

Metadata .csv Formatting

Example configuration of a Metadata Watch Folder:
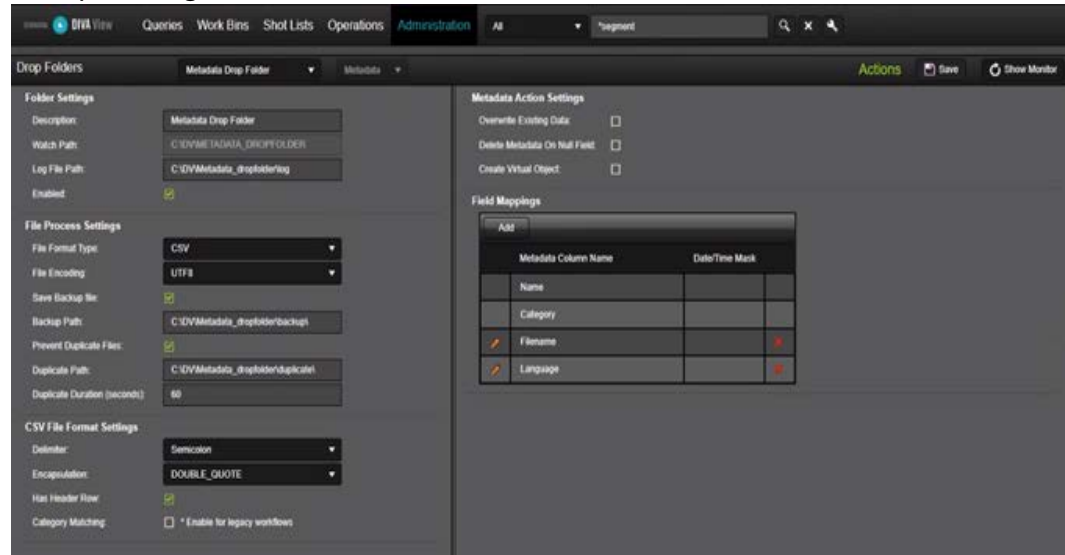
Example of the corresponding Metadata File that will be dropped in the Metadata Watch Folder:

In the Watch Folders configuration screen, one can also view the history log for each configured Watch Folder:
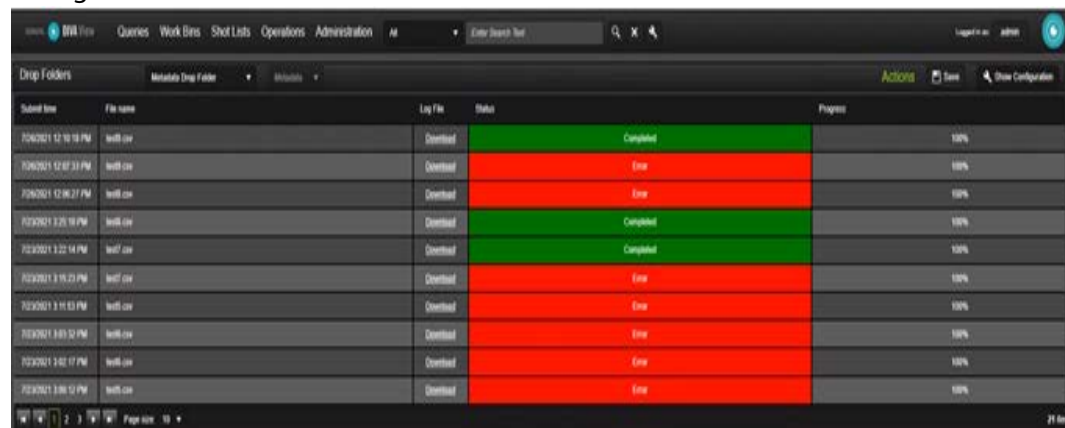
The log File contains the results of the processing of each dropped Metadata File:

Metadata XML Formatting

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

The following example shows the required XML formatting:

```xml
<?xml version="1.0" encoding="utf-8"?>
<DIVAViewMetadataXML>
    <Category object_category="str1234">
        <Object object_name="str1234">
            <Item metadata_name="str1234" dt_mask="str1234">
                <Value>str1234</Value>
            </Item>
            </Item>
        </Object>
    </Category>
</DIVAViewMetadataXML>
```

Logging Configuration

There are three important sets of log files used in DIVA View:

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

All DIVA View logs aggregate on the same UDP port (7071 by default) and can be monitored by Log4Net compliant logging applications to provide live system monitoring. For DIVA View 6.1.0.209 you should use the log4view application, which is downloadable here: https://www.log4view.com/download-en. However, these logging applications are extremely resource intensive and should not be left running in the background.

The <log4net> section of the file named:

```
C:\Program Files (x86)\EcoDigital\DIVAView\www\Web.config
```

controls the contents of:

```
C:\Program Files (x86)\EcoDigital\DIVAView\www\logs
```

The file is editable using a plain text editor (such as Notepad or Notepad++); do not use an editor that adds formatting (for example, Microsoft Word).

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

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

telestream

```
        <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 Technical Support.

  – DEBUG

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

  – INFO

    At this level only informational messages, warnings and errors are collected. This setting enhances performance for the site, UDP throughput, and log file reporting. Technical recommends using this as your Network 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 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.

DIVA View 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 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 file named:

`C:\Program Files (x86)\EcoDigital\DIVAView\www\Web.config`

DIVA View Task Manager Logging Configuration

The Task Manager logs contain information regarding scheduled tasks, including Watch Folder operations, synchronization, request updating, and housekeeping, among others (see *Task Manager and DIVA View API Windows Services* for more information).

The Task Manager logs are located in:

`C:\Program Files (x86)\EcoDigital\DIVAView\TaskManager\logs`

The configuration for these log files is located in:

`C:\Program Files (x86)\EcoDigital\DIVAView\TaskManager\log4net.config file`

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

DIVA View API Logging Configuration

The API logs contain information regarding user log in.

Note: The Client Uploader is no longer supported starting with release 6.0.

The API logs are located in:

`C:\Program Files (x86)\EcoDigital\DIVAView\Api\logs`

telestream

The configuration for these log files is located in the file named:

```
C:\Program Files
(x86)\EcoDigital\DIVAView\Api\Telestream.DIVAdirector.Api.log4net.
config
```

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

Default Configuration File

The following is the default configuration file included with the DIVA View distribution.

```
{

"QuietInstallation": false,
"InstallType": "CleanInstall",
"DDApiUrl": "https://DV6:6543",
"DDApiIpAddress": "127.0.0.1",
"HostName": "DV6",
"ServiceUserName": "dv6-user",
"DefaultServicePassword": "Contact Telestream Support",
"UpgradeDirectory": "C:\\Program Files
(x86)\\EcoDigital\\__DDUpgrade__",
"LicensePath": "C:\\Program Files
(x86)\\EcoDigital\\www\\DIVAView.licx",
"BackupDirectory": "C:\\Program Files
(x86)\\EcoDigital\\__DDBackup__",
"InstallationDirectory": "C:\\Program Files
(x86)\\EcoDigital\\DIVAView",
"DIVAconfiguration": {
  "Url": "http://10.0.0.0:9443/diva/service/rest/2.2/
DIVArchiveWS_REST",
  "ApiKey": "replace_with_api_key",
  "ClientId": "replace_with_api_key"
},
"WebConfiguration": {
  "StorageLocations": null,
  "SearchLanguage": null,
  "NumConcurrentUsers": 0,
  "ExternalDomainUrl": null,
  "ProxyStoragePath": "H:\\DIVAView Proxies",
  "DatabaseBackupPath": "H:\\DIVAView Database Backup",
  "LocalArchivePath": "H:\\DIVAView Local Archive Source",
  "LocalRestorePath": "H:\\DIVAView Local Restore Destination",
  "QCPath": "H:\\DIVAView QC Report"
},
"InstallTranscodeService": false,
"DatabaseImportPath": null,
"DatabaseVersion": null,
"DataDirectory": "H:\\DIVAView Database",
"DatabaseInstallationDirectory": "C:\\Program Files
(x86)\\EcoDigital\\DIVAView\\Postgres",
"EnableCommentFilenameValidation": false,
```

```
"EnableLocalRestoreNameConversionFromMetatype": false,
"AllowNewInstanceSynchronization": false,
"TranscodeServiceUsername": null,
"TranscodeServicePasswordEncrypted": null
}
```

Synchronization Task for Complex Objects and Logging

The following keys can be added to the configuration file for various synchronization tasks. Only the SkipComplexObjectSync parameter is added by default. The other parameters must be added manually.

```
<!-- DIVArchive client settings - END -->
<add key="SkipComplexObjectSync" value="false" /> <!-- This flag
sets whether or not to sync the entire complex object file list (it
is required that this be set to true when using the legacy WSAPI
due to limitations in the API. Sometimes it will work, but often it
will not.) -->
<add key="SanitizeDIVArchiveResponses" value="false" /> <!-- This
flag sets whether or not attempt to clean poorly formatted XML in
comments field (this is automatically done in EC, but may need to
be added when using WSAPI) -->
<add key="LogDIVArchiveResponses" value="false" /> <!-- This flag
sets whether or not log each GODL request -->
<add key="LogDIVArchivePath" value="<Some Path to Log>" /> <!--
This flag sets whether or not log each GODL request -->
```

Optional Manual Adjustments

This section describes instructions for adapting the system if it is getting short on disk space.

Using NAS (Network Attached Storage) for Proxy File Storage

The Proxy File Storage Folder may become very large. You can place it on internal Server Storage or on an external (larger) NAS (Network Attached Storage) array. You must add new Proxy Storage Location pointing to a Shared Network Folder.

The Network Path must be specified in the following UNC format:

```
\\host_name\share_name\subfolder\...\subfolder
```

The Microsoft Windows Local System account is restricted from accessing network resources. Therefore, you must use a dedicated user account instead. You must grant access rights to read the Proxy folder on the NAS to the same account. You must configure the Proxy folder to allow the user account running the IIS application pool and the DIVA View Task Manager to write to the Proxy folder.

You must grant this account read and write permissions for accessing the Proxy folder on the NAS, and the user account running the DIVA View Web Server service must be a member of the Administrators group because typically this service must have access to the Program Files folder. You must also add the account to the IIS_IUSRS group to run the IIS application pool.

Using a path with a mapped drive letter (for example K:\Proxies) is not supported because this path will be used by the DIVA View Web Server for opening proxy files upon user requests. The Web Server that runs as a service is not aware of mapped network drives because these are associated with an interactive user session.

Note: DIVA View Proxy storage can also be on a SAN. However, some SANs do not have drivers that are fully compatible with IIS and cannot be used for this purpose.

PostgreSQL SSPI Pass-Through Authentication Setup

PostgreSQL SSPI Pass-Through Authentication can be set up after DIVA View is upgraded if you are using the same domain user account to run all DIVA View services, the IIS application pool, and PostgreSQL. This configuration removes the need to have plain text user names and passwords in the connection strings, providing improved security.

Follow the instructions to enable SSPI for PostgreSQL at:

https://wiki.postgresql.org/wiki/Configuring_for_single_sign-on_using_SSPI_on_Windows.

After you complete the instructions, you must update the configuration files for each of the following DIVA View services. You must modify the configuration files in the following default locations:

- DIVA View Web Service

  ```
  C:\Program Files(x86)\DIVAView 6\www\Web.config
  ```
- DIVA View TaskManager

  ```
  C:\Program Files (x86)\Divaview
  6\TaskManager\Telestream.DIVAView.TaskManager.exe.config
  ```
- DIVA View API

  ```
  C:\Program Files (x86)\Divaview
  6\Api\Telestream.DIVAView.Api.exe.config
  ```
- DIVA View Annotation Import Service

  ```
  C:\Program Files (x86)\Divaview
  6\Tools\DVServices\DIVAViewServices.exe.config
  ```

  In each of the services the key will be the same:

  ```
  <connectionStrings>
      <add name="DIVAViewContext"
  connectionString="Server=localhost;Database=DIVAView;User
  Id=postgres;Password=MANAGER;" providerName="Npgsql"
      />
  </connectionStrings>
  ```

  The connection string parameter must be modified as follows:

  ```
  connectionString="Server=localhost;Database=DIVAView;Integrated
  Security=true;Include Realm=true;"
  ```

Configuration for ShuttlePro V2 or ShuttleXpress Control Pads

Install and configure Contour's control pad on the 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)\DIVA View 6\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)\DIVA View 6\Support\etc\Pref file - Mac\com.contourdesign.shuttle.prefs`

    to

    `~/Library/Preferences/`

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

telestream

Glossary

Annotation

An annotation is additional information associated with a file clip or object. It can be a note that includes a comment or explanation.

API Service

An API Service is a web service that allows two applications to talk to each other. It is typically responsible for handling authentication, authorization, file transfer jobs, and so on.

Complex Object

A complex object contains 1,000 or more files. This value is configurable in DIVA Core. Complex object handling may be different than non-complex objects. See **Virtual Object**.

Data Store

A data repository of a set of integrated objects.

Watch Folders

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

IIS (Internet Information Service)

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 System Management App.

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.

Virtual Object

Virtual Objects are archive entries. An Virtual Object (archive entry) is identified by a pair (Name and Collection) and contains video files, audio files, metadata files, and so

on. The files are stored in DIVA Core as Virtual Object Instances. An Virtual Object can contain up to 1,000 files before being considered a complex Virtual Object. See **Complex Object**.

PFR (Partial File Restore)

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

Profile

In DIVA View the User Profile is where the user can configure their own account settings (to some extent). Some settings are non-configurable by the user and are configured by the System Administrator. The user settings are also restricted by the Organization and Group settings that the user is a member of. Users can change name, email, phone number, and so on in their profile.

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. Proxies are stored in DIVA View Proxy Locations, whereas source files are archived in DIVA Core.

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.

System Metadata

System Metadata is preconfigured in DIVA View and is valid for all Organizations, Groups and Users. System Metadata cannot be deleted or changed.

Task Manager

Task Manager is a Windows feature that provides details about programs and processes running on your computer. It also displays the most commonly used performance measures for processes. Using the Task Manager can provide you with details on current programs. You can start, stop, enable and disable individual tasks and programs through the Task Manager interface.

Thumbnails

Thumbnails are small image representations of a larger image, usually intended to make it easier and faster to look at or manage a group of larger images.

Transcode Service

Transcoding is the process of converting an audio or video file from one encoding format to another. The Transcode Service is the Windows service that handles the transcoding jobs.

telestream

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.

User Metadata

User Metadata is configurable by the administrator and also by the user. When configured by the administrator it is applicable to all users in the system. When configured by the user it is applicable only to the user unless they share the metadata with their Organization or Group.

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.