



EVS IP DIRECTOR LOGS PROCEDURE

Prerequisites:

- Use our Web portal to enter a new issue, and fill out all fields required. Always indicate the client workstation (name, IP address, serial number) and user role.
- **Do NOT** use 7z or other zipper. Use classic Windows zipper to zip the logs directory.
- Follow the procedure according to the product below to collect their respective logs files.
- If the problem can be easily reproduced, it will be better to backup all logs, then flush the entire C:\EVSLogs directory (EVS Services must be stopped). The biggest advantage will be to have smaller logs and easier to analyze.
- If you suspect a memory leak, please use "Procdump.exe" and collect Windows event logs entries. The usage is described in this document.
- Always indicate a timestamp when the error occurred and a print screen of the error. If the problem happened systematically please include with the logs a short Video showing the problem and steps to reproduce it.



IP DIRECTOR LOGS PROCEDURE

IP Director:

In order to collect log files you need to log on the Remote Installer with “Administrator” account.

In any cases logs must be collected from IP Director with its SynchroDB running in Master Candidate and from SynchroDB managing Video Servers, Nearline getting problems.

1. If SynchroDB are configured in Network mode:

Video Servers:

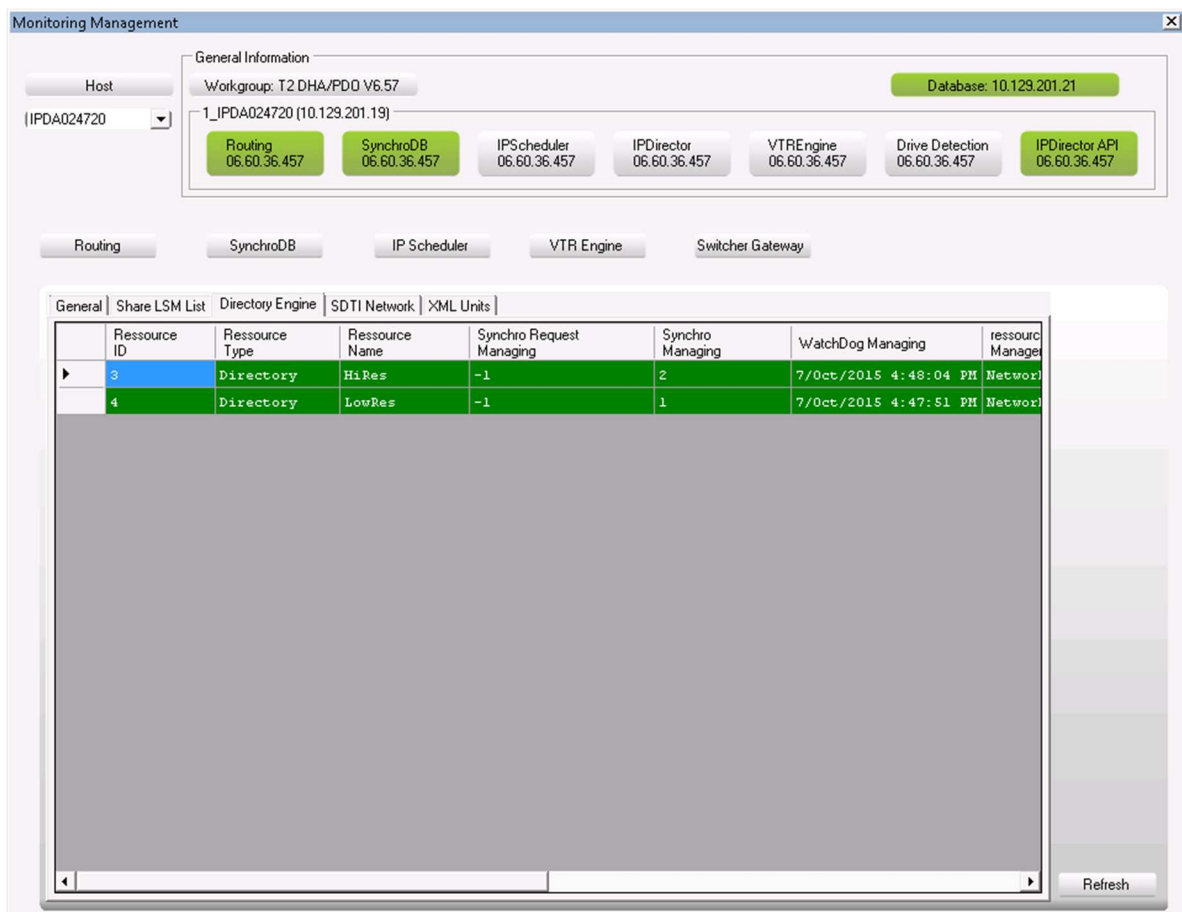
- a. Open the Monitor software from SynchroDB service.
- b. From “Share LSM List” tab:
 - a. Check from “SynchroDB Managing” column the “Local machine number”
 - b. From the Remote Installer retrieve log file from the IP Director with this “Local machine number”

The screenshot shows the 'Monitoring Management' application window. The 'Share LSM List' tab is active, displaying a table with the following data:

ID Lsm	Resource Name	ID Managing	Via SDTI	Num User	ID SynchroDB	Synchro Managing	Management Status
23670		23670	False	1		1	Do Not Update
148820		148820	False	2	00:03:1D:0E:5C:08	2	Up To Date

Nearline:

- a. Open the Monitor software from SynchroDB service.
- b. From “Directory Engine” tab:
 - a. Check from “SynchroDB Managing” column the “Local machine number” to isolate the SynchroDB managing the server.
 - b. From the Remote Installer retrieve log file from the IP Director with this “Local machine number”



2. If SynchoDB are configured in Restricted Stand Alone mode:

- . Retrieve log files from the Master Candidate SynchroDB
- . Retrieve log files from the SynchroDB managing the server

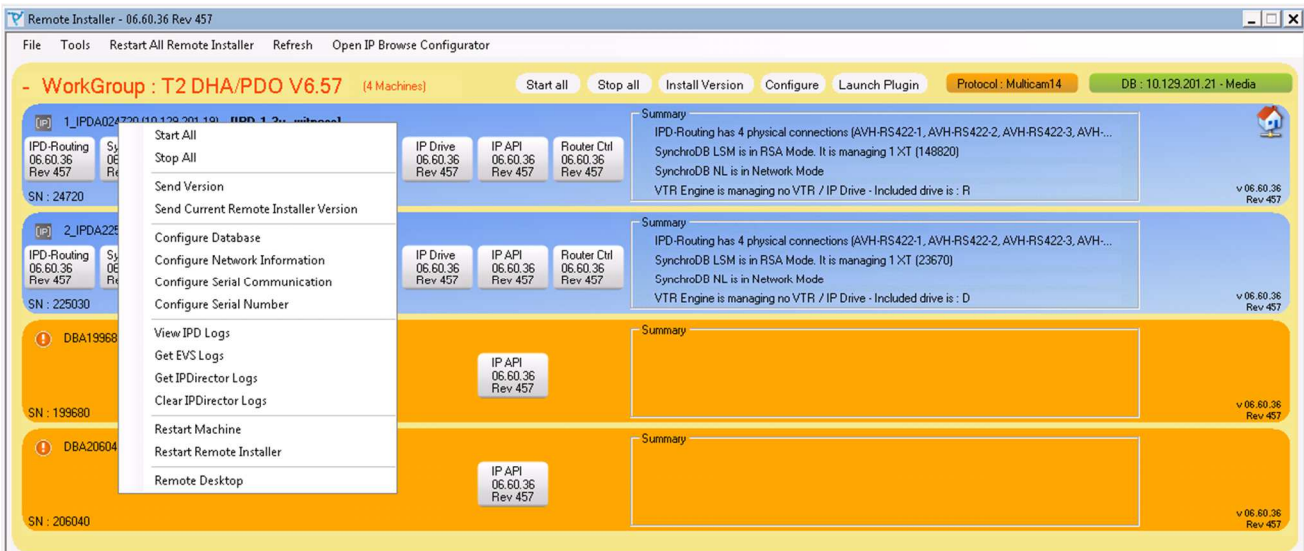


IP DIRECTOR LOGS PROCEDURE

How to get logs:

Right click on the computer name managing the Video Server or Nearline and choose “Get EVS Logs”.

If possible please stop all services before extracting logs.



If SynchroDB are set in Restricted Standalone mode:

Grab log from the IP Director with its SynchroDB managing this Video Server or Nearline.

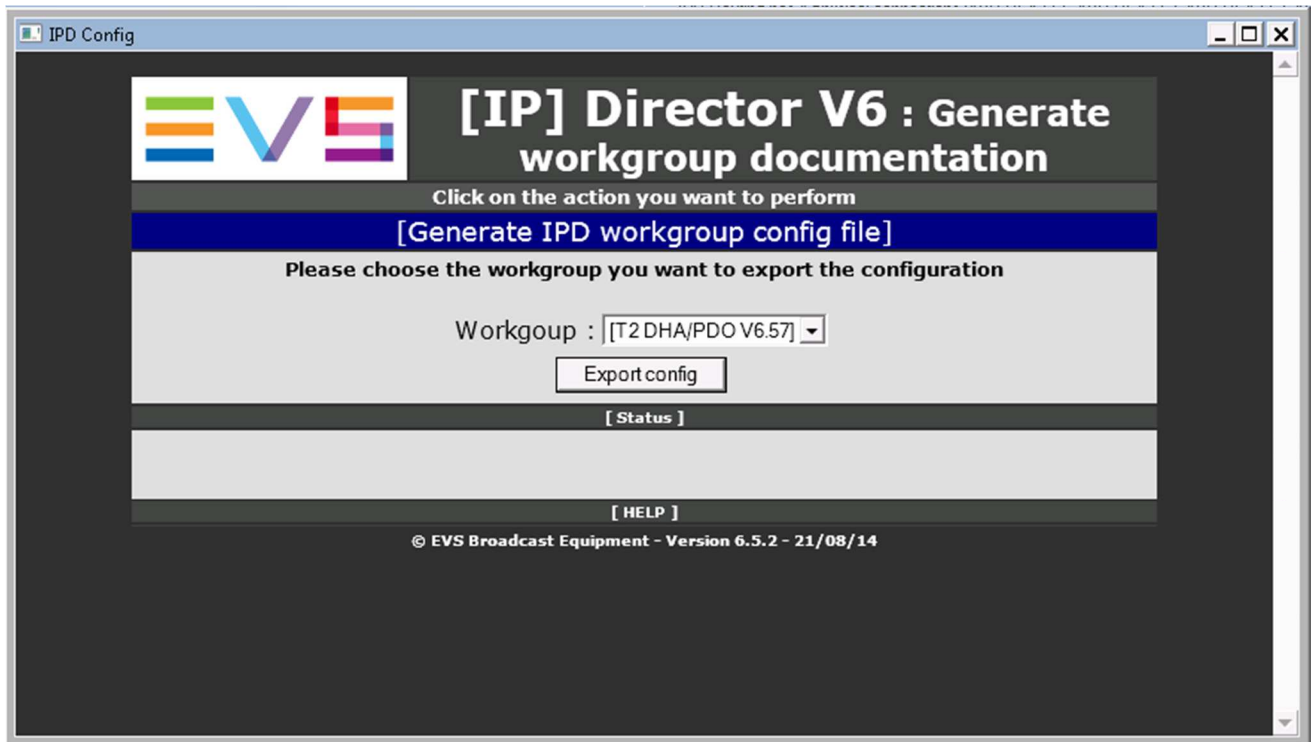
If possible please stop all services before extracting logs.



IP DIRECTOR LOGS PROCEDURE

Workflow:

The entire workgroup description must be grab using “[IP] Director_6_ConfigGenerator.hta” Plugin.



IP Director – Video Server:

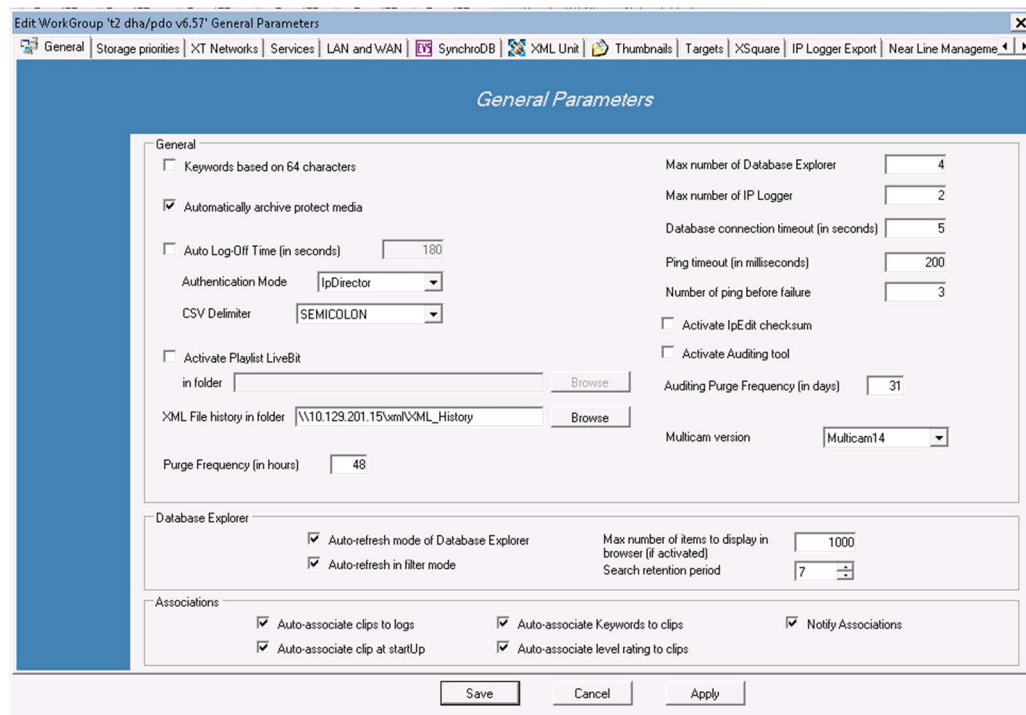
Could you please provide the RS-422 connection diagram between IP Directors and Video Servers?

Extra logs to be provided with specific cases:

Media Transfer issue:

When transfer issue happened please provide IP Director “XML File History” will also be mandatory to track jobs errors between IP Director and XSquare.

Please zip the entire content from the defined directory in IP Director -> Configure -> General Parameters -> XML File History.



Restore Play List Elements to Server:

- Provide the History job XML IPD.
- Playlist ID and screenshot.
- XSquare Logs DB + XSquare DB if possible
- XTAccess job processor + EVSLogs XTA

Communication problem with Video Servers:

- Collect Video Server connected by RS-422 to the IP Director.

Router Control:

- Be sure you are providing logs from the Master Router Control service (see the green bold one in Remote Installer)



IP DIRECTOR LOGS PROCEDURE

Playlist Linked with MOS:

- Provide playlist ID and screenshot.
- Collect logs from the XS server involved
- Collect log from the Mos Gateway computer. Zip the entire C:\EVSLogs directory
- Collect logs from computer running API service in master mode (see the green bold one in Remote Installer).

Asset Coherence Break:

- Check if one message on the Video Server OSD !TC . If yes please Resync the incoming time code on this particular video server. Save the stream in a clip and try to transfer it.
- Provide clip name in Ingest scheduler
- Collect logs from the IP Director managing Near Line(s).
- Collect XSquare logs + the one from XTAccess jobs processors

Nearline Management:

- Verify if DB status from its monitoring page. (if your setup use Database servers).
- Collect logs from IP Director managing Video Servers and Nearline.

Playlist nothing changes and lines in italic:

- Collect logs from IP Director managing Video Servers and Nearline.

IPWeb:

- Zip the entire C:\EVSLogs directory from the IP Director Web server.
- Zip the entire C:\EVSLogs directory from the Workflow Manager



How to use Procdump.exe

Procdump.exe is a software from Microsoft to be used to collect a dump file upon application crash

How to collect a dump file upon application crash.

If a software is generating .dmp files and if the R&D is complaining that the dmp file is not complete enough, you may use the procdump.exe to generate a full dmp file.

Procdump.exe software can be downloaded from: <http://technet.microsoft.com/en-us/sysinternals/dd996900>

_ Copy procdump.exe anywhere on the machine (eg: C:\Temp\procdump.exe).

_ Launch procdump.exe with the right arguments: `procdump.exe -e -ma -o -w application_name.exe dump_file.dmp`

Arguments details:

-e Write a dmp when the process encounters an unhandled exception

-ma	Write a dmp file with all process memory
-o	Overwrite the dmp if it exists
-w	Wait for the process if it does not already exists
-accepteula	Automatically accept the Sysinternals license agreement

i.e. with XTAccess application:

`procdump.exe -e -ma -o -w xtaccess.exe C:\EVSLogs\XTAccess\XTAccess_procdump.dmp`

_ Launch the application and try to make it crash.

_ once the crash happened, collect the generated dmp file



IP DIRECTOR LOGS PROCEDURE

If the R&D is asking a dmp file of a running application, you may use the procdump.exe to generate a full dmp file.

The procedure will be the same as described before:

_ Copy procdump.exe anywhere on the machine (eg: C:\Temp\procdump.exe).

_ Launch procdump.exe with the right arguments.

I.e. xtaccess.exe

```
procdump.exe -ma -o -w XTAccess.exe C:\EVSLogs\XTAccess\XTAccess_procdump.dmp
```

Corporate

Headquarters
+32 4 361 7000

North & Latin America

Headquarters
+1 947 575 7811

Asia & Pacific

Headquarters
+852 2914 2501

Other regional offices

Available at
www.evs.com/contact