



EVS XSQUARE LOGS PROCEDURE

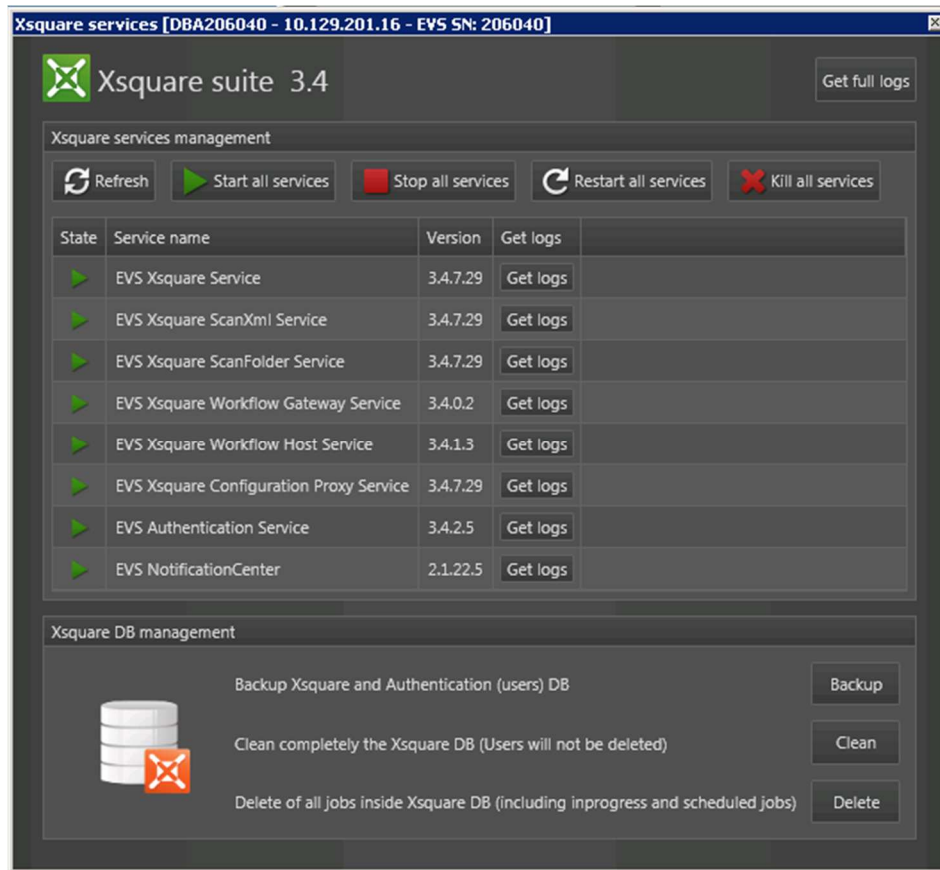
Prerequisites:

- 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.



Xsquare:

- Collect logs from XSquare
Open XSquare services monitoring window and click on “Get full logs” button.



- Please provide also XSquare database in case of issue when processing jobs from IP Director, SOAP or third party software.
- Backup can be initialized from the XSquare Services software by clicking on the “Backup” Button.



- 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.



XTAccess:

- If the problem is localized from **one** particular XTAccess computer you will be obliged to stop XTAccess and XTGateway softwares and zip following directories from the XTAccess computer: C:\EVSLogs\XTAccess C:\EVSLogs\XTGateway.
- XTAccess managing the job can be easily found from the XSquare monitoring window by double clicking on the failed jobs. The processing device name will be showed and you will be able to get logs from it.

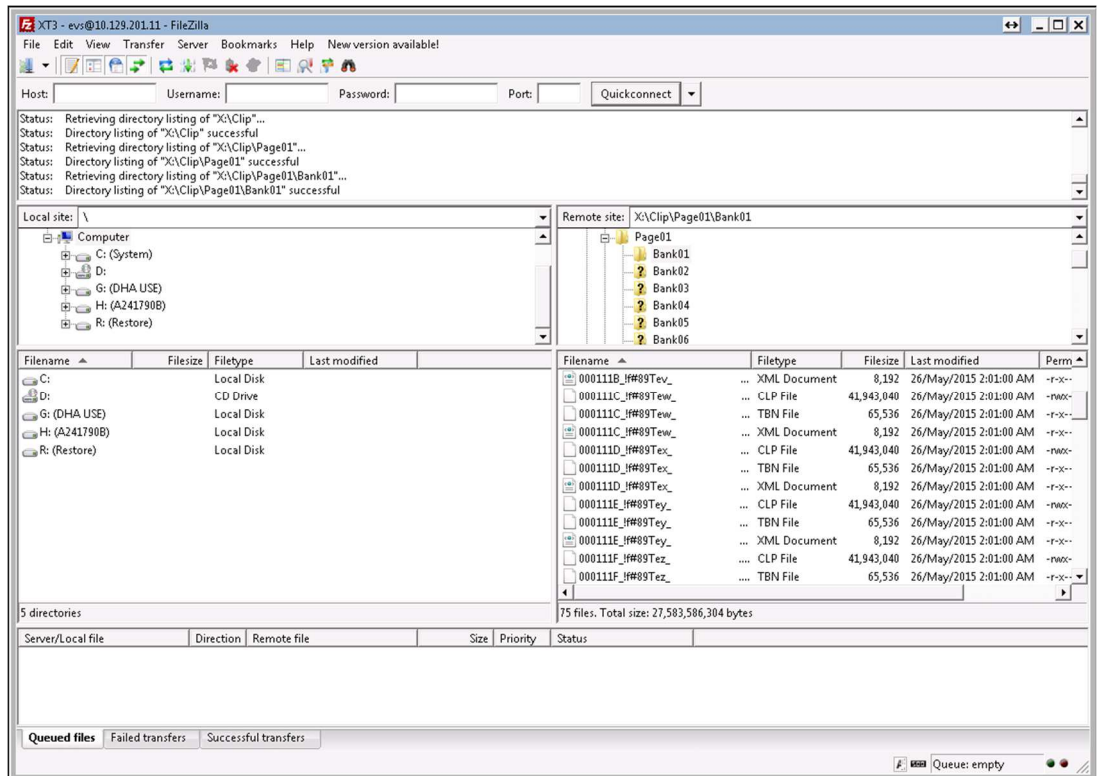
The screenshot displays the XSquare monitoring interface. The top section shows a table of jobs with columns for ID, Status, Received date, Job Type, Source Type, Frames/s, Mbytes/s, XTA Nickname, Dest Clip Name, Source Path, Source Name, Source Clip Name, Message, and Initiator. Job ID 933003 is highlighted in red. Below the table, a detailed view for job ID 933003 is shown, including fields for Username (Administrator), Source Path (10.208.116.11 - 10.208.120.11), Received date (24/10/2013 15:56:38), Initiator (IPDirector 6.40.12), Source Name (000A), Start date (24/10/2013 15:56:43), Job Type (train), Source Clip Name (XS01-IN1), End date (24/10/2013 15:58:31), Job Type (Transfer), Src. VarID (45D06+H), Src. UID (45D06+H), Last notification date (24/10/2013 16:08:28), Receiver (LMD Nearflow), Source code (Apple Profax 42), Cluster (XS 1), Current TC (18:07:17:03), Frames/s (26.18), Mbytes/s (18.23), XTA location (L-XTA-ING-02), XTA Nickname (L-XTA-ING-02), and Processing Device (L-XTA-ING-02 XTAccess v.2.2.7.17 (SR-17350)). The bottom section shows a table of failed status entries with columns for Status, Destination, Dest Clip Name, Destination Code, Message, and Transcoding EDI destination. Three entries are listed, all with a status of 'Cancelled' and a message of 'Destination cancelled.' The 'Message' column in this table is circled in red.

- If the problem happened with one media **file** please provide it.



XSQUARE LOGS PROCEDURE

- If the problem happened with one Video Server clip: Connect over Gige Video Server interface using its ftp server using [Filezilla](#).
Host: Video Server IP Address
User: evs
Password: evs!
Directory: please browse Video Server content using LSM ID from the faulty clip.
Download both i.e. LSM ID: 111B -> 00011B_.....XML and 00011B_.....CLP files.



- If the problem happened from the record train: Please create one small clip with the problem and backup its .clp and .xml file using [Filezilla](https://filezilla-project.org) (https://filezilla-project.org).



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

```

Scroll Administrator: C:\Windows\system32\cmd.exe
Press Ctrl-C to end monitoring without terminating the process.
The process has exited.

C:\>procdump.exe -e -ma -o -w CleanEdit.exe C:\EvsLogs\CleanEdit\CleanEdit_procdump.dmp

Procdump v5.13 - Writes process dump files
Copyright (C) 2009-2013 Mark Russinovich
Sysinternals - www.sysinternals.com
With contributions from Andrew Richards

Waiting for process named CleanEdit.exe...

Process:                CleanEdit.exe (4556)
CPU threshold:          n/a
Performance counter:    n/a
Commit threshold:       n/a
Threshold seconds:      n/a
Number of dumps:         1
Bug window check:       Disabled
Exception monitor:      Unhandled
Exception filter:        Disabled
Terminate monitor:      Disabled
Dump file:               C:\EvsLogs\CleanEdit\CleanEdit_procdump_VVMMDD_HHMMSS.dmp

Press Ctrl-C to end monitoring without terminating the process.
[09:39:35] Exception: E06D7363.70UExceptionPstrd@
[09:40:03] Exception: C0000005.ACCESS_VIOLATION
[09:40:03] Exception: Unhandled - C0000005.ACCESS_VIOLATION

Unhandled Exception.
Writing dump file C:\EvsLogs\CleanEdit\CleanEdit_procdump_130418_094003.dmp ...
Writing 235MB. Estimated time (less than) 7 seconds.
Dump written.

The process has exited.

C:\>_

```



XSQUARE 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