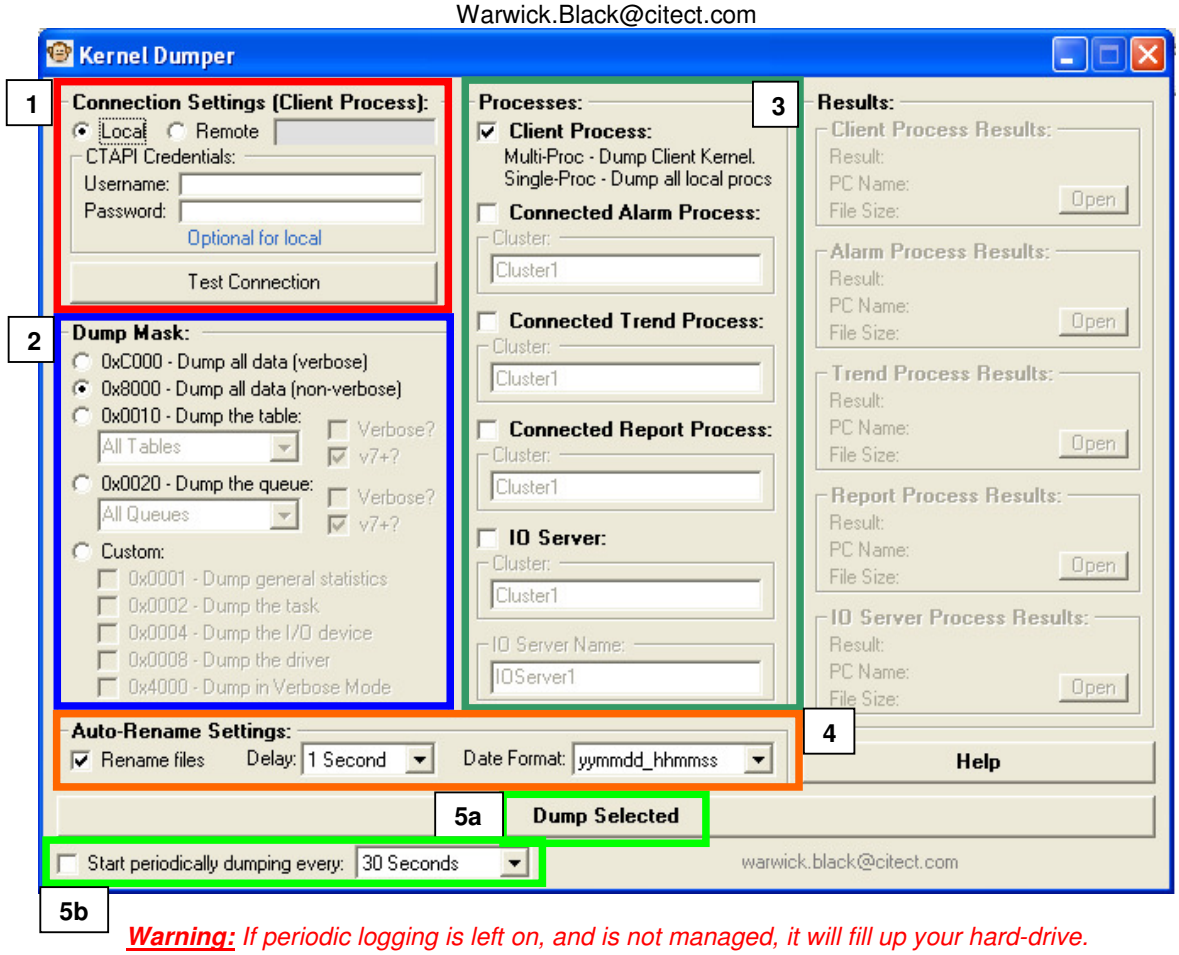
Kernel Dumper Help

Warwick.Black@citect.com



Warning: *If periodic logging is left on, and is not managed, it will fill up your hard-drive. The filesize for each log is shown, in order to assist you in tuning your periodic logging + HDD usage.*
Kernel Dumping will put additional load on your SCADA system, and will block execution of tasks and cicode, it is not recommended to Dump unnecessarily – But is useful for debugging purposes

Overview

Kernel Dumper is a utility that connects to Citect SCADA via CTAPI, and can issue commands to trigger 'Dumping' of the Citect Kernels.

As the Kernel Dumper connects to the CTAPI connection in the Client Process, commands are issued through the Client, and passed on to the relevant Process, which may or may not be local to that Client PC.

Usage:

This application is stand-alone, it contains all required Dlls, and can be run from anywhere, i.e it does not need to be placed in the BIN directory.

1. Complete Connection information, pointing to the target Client Process
    a. Username and Password is optional for a local connection.
    b. For a remote connection, use a configured Citect SCADA Account.
2. Configure the 'Dump Mask' that will be used for all targeted processes
3. Select and configure the Target Processes
4. Edit whether you want all logs in the one file, or to rename the file each time, with Date/Time stamps

5a. Perform a 'One-off' Kernel Dump
5b. Perform periodic logging at the specified rate

Log files are created on the Process Host machine, in the 'LOGS' folder (or pre v7 in C:\Windows)

Periodic Logging:

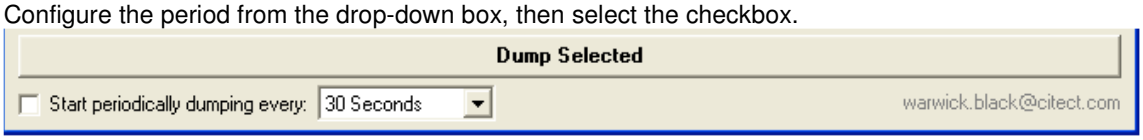
Periodic logging can be used to trace 'Leak' type issues, where periodic Kernel Dumps can shed some light on what values could be increasing without ever freeing up.

To configure, simply ensure all the other options have been filled out correctly, and instead of hitting the 'Dump Selected' button, select a time period, and tick the checkbox.

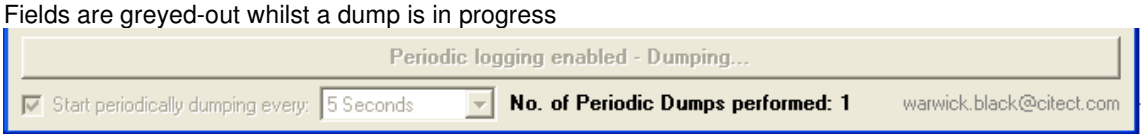
1 dump will be performed straight away to ensure there are no errors in the configuration, then a countdown will start till the next Dump is performed. "Kernel Dumper" must stay open for the Periodic dumping to occur.

Periods can be from 1 second, to 24 days.

Configure the period from the drop-down box, then select the checkbox.

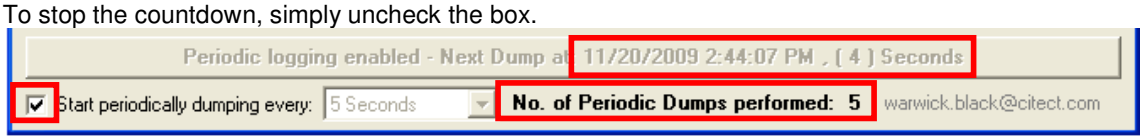


Fields are greyed-out whilst a dump is in progress

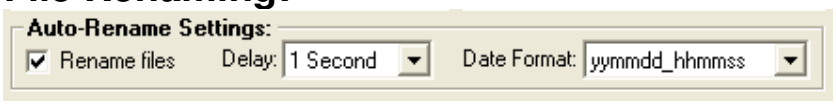


Once the dump is created, the countdown starts till the next dump, and the date/time of the next dump is displayed. There is also a counter of how many period logs have been created in that current session.

To stop the countdown, simply uncheck the box.



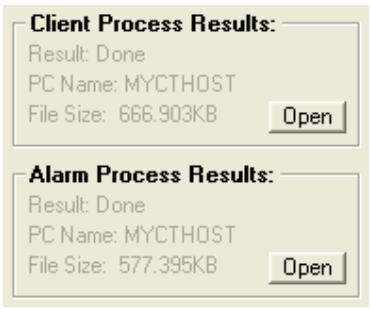
File Renaming:



These options determine whether the Kernel.Dat files are renamed after each Dump is performed. By default this is enabled, and the date/time is appended to each file, in the format: **yymmdd_hhmmss**, which is: Year Month Day _ Hour Minute Second.

There are 3 other options provided:
yyddmm_hhmmss, which is: Year Day Month _ Hour Minute Second
hhmmss_ yymmdd, which is: Hour Minute Second _ Year Month Day
hhmmss_yyddmm, which is: Hour Minute Second _ Year Month Day

Results:



The Results form only holds the results for the **last round** of Dumps.

Result - Possible values:
Done – Done, no errors
Done – Single Proc? – Done, might be in Single Process and only need to Dump the Client
Error – Failed, refer to pop-up message for further info.

PC Name: The name of the Host of the Dumped Process
File Size: The Size of the file created on the Host PC
Use this Filesize to determine how much HDD space will be used in Periodic logging.

Troubleshooting / Logging:

In the Kernel 'Main' window, and the Syslog.dat file, there will be a message when a "Kernel Dumper" is about to request a Dump, and after the Dump has completed running.

The PC name of the machine that is running "Kernel Dumper" is posted in this log, in order to determine where the request is coming from, to assist in debugging.

```
2009/11/19-03:00:54.250 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:00:55.281 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
2009/11/19-03:14:26.093 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:14:27.250 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
2009/11/19-03:14:34.375 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:14:35.515 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
2009/11/19-03:26:02.484 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:26:03.546 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
```

syslog.dat - Notepad

File Edit Format View Help

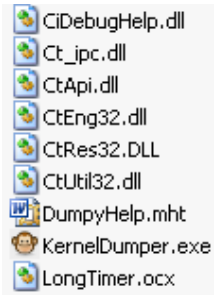
```
2009/11/19-03:00:54.250 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:00:55.281 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
2009/11/19-03:14:26.093 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:14:27.250 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
2009/11/19-03:14:34.375 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:14:35.515 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
2009/11/19-03:26:02.484 ***KERNEL DUMPER*** Cluster1.Client- START Dump, from: CITECT-91397D34
2009/11/19-03:26:03.546 ***KERNEL DUMPER*** Cluster1.Client- FINISHED Dump
```

CTAPI debugging can also be used to see the incoming messages/requests.

Installation Package:

The installation package is a SFX or self-extracting ZIP file. It is configured to extract all files to a *TEMP* directory, then run the main EXE.
CTAPI is backwards compatable with all SCADA versions, and the CTAPI Dlls from 7.10 SPK1 are packaged inside this SFX. However, if you are having compatabilty issues, the KernelDumper.EXE file can be extracted from the SFX, and placed in the Bin directory of your older (or newer) SCADA system.

The files contained in the SFX ZIP are:



The Ci* and Ct* files are the Citect 7.10 SPK1 CTAPI files that the application is dependant upon. The LongTimer.OCX is an ActiveX control that is required to obtain the 24 day Timer functionality used in Periodic Logging.

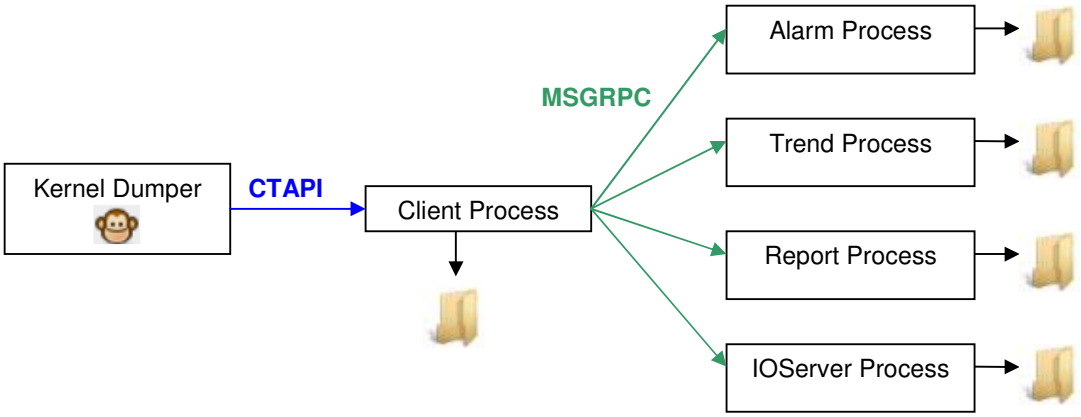
Technical Notes

How it works:

As the Kernel Dumper connects to the CTAPI connection in the Client Process, commands are issued through the Client, and passed on to the relevant Process.

As a result, only access via CTAPI to the SCADA system is required, additional windows networking settings are not necessary (but can be implemented to assist remote opening of the logs – discussed later).

If using this tool remotely on a 7.10+ system, you must set [CTAPI]Remote=1 on the target Client PC.



Single-Process Considerations:

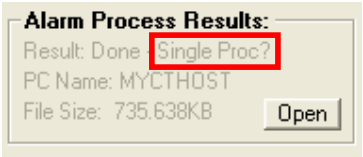
When Citect is run in Single-Process Mode, to dump all current processes running on the target Client, simply dump the 'Client' process. This is because, in Single Process, there is only one Citect Kernel, regardless of how many processes are running on that PC.

When Citect is in Single Process, If you dump Processes other than the Client, the dumps should all be identical to the Client Dump, *UNLESS* the Processes are not on that local machine, in which case, it will send the commands to the currently connected server of that type.

The dump files are always created locally on the machine that hosts the process, to prevent confusion. After each Dump, the Kernel files are always renamed with the Date and TimeStamp.

Currently, the TimeStamp issued is the current time of the machine where "Kernel Dumper" is running. This helps when trying to coallate Dumps from multiple machines for the same time.

In the 'Results' field, you will see the following message if "Kernel Dumper" determines you might be dumping multiple Kernels in single process, using uneccesary HDD space with identical logs.



Multi-Process Considerations:

In Multi-Process mode, you must select each process you wish to dump. However, note that the Client on a Server is not forced to talk to it's own Servers. i.e The dump commands will be sent out to the currently connected Process of the correct type, which may/maynot be local to that PC.

The PC Name is provided in the results field to give an indication of where the log files are, and the 'open' button will attempt to open the created log files, however may not be successful depending on your network rights.

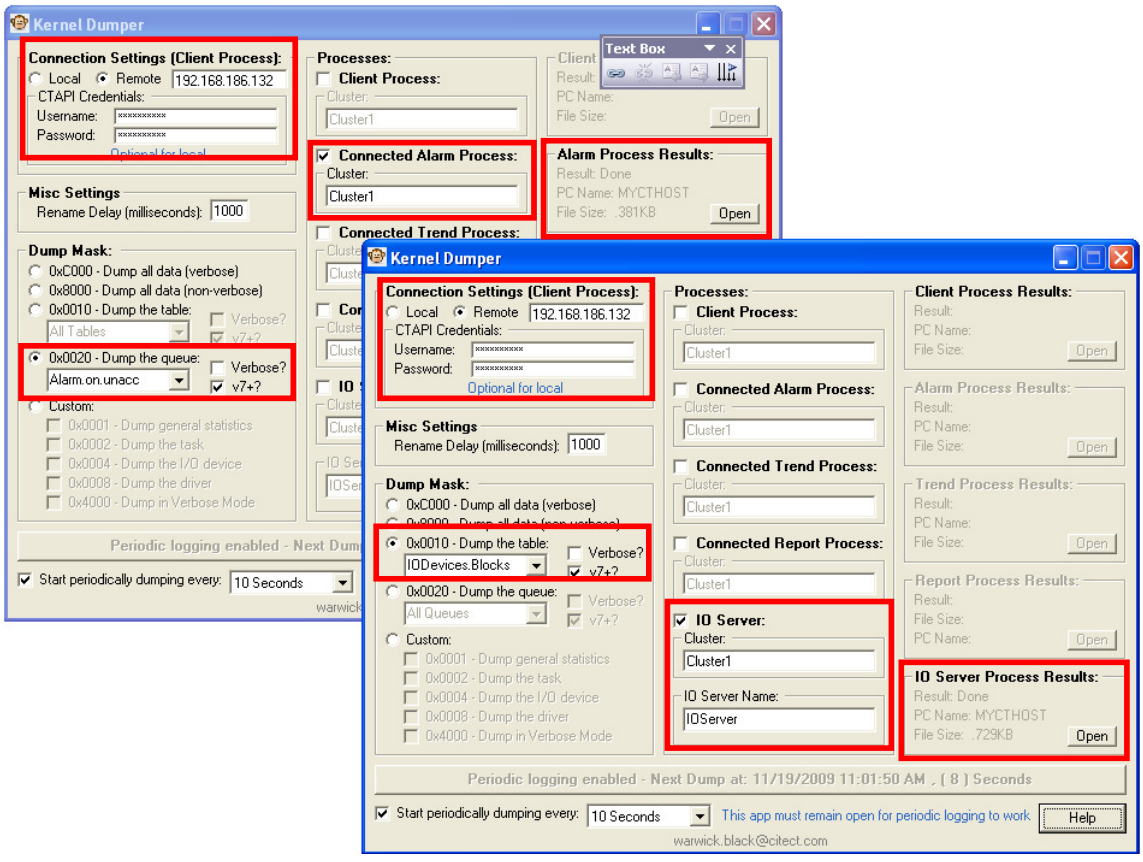
Multiple Instances:

In order to simplify the application, there is only the option of configuring one mask per "Kernel Dumper" instance.

However, with care, multiple instances of the Kernel Dumper can be run on the same system with different masks.

Rule of thumb: Don't configure multiple instances of "Kernel Dumper" to the same Process.

- If you are not careful with the timing of these instances, it will result in file-access issues as they will be trying to write / rename the same Kernel.dat file
- Likewise, multiple "Kernel Dumper" sessions pointing to Citect running in Single Process mode, with all the processes on the same SCADA machine will all be trying to write / rename the same Kernel.dat.



Above: *Multiple instances of "Kernel Dumper" running periodically on the same target Client, for different processes, with different masks.*

1st: *Is Dumping the 'Alarm.on.unacc' Queue from the Alarm Server every 10 seconds*

2nd: *Is dumping the 'IODevice.Blocks' Table from the IOServer every 10 seconds*