

# *AccessData Oradjuster*

AccessData **Oradjuster.exe** optimizes certain settings within the AccessData Oracle database, and this allows FTK to achieve peak performance during investigative analysis. This utility is particularly useful for 64-bit systems with large amounts of RAM on board. It is included in the FTK 3.1 Database install disc.

This document describes Oradjuster's role in making maximum use of AD Oracle. To see a webinar that demonstrates Oradjuster, look under the Core Forensic Analysis portion of the web page: <http://www.accessdata.com/Webinars.html>.

## **ORADJUSTER SYSTEM REQUIREMENTS**

Oradjuster operates on all FTK supported Windows platforms (both 32 and 64-bit) where AD Oracle has been installed.

## **INTRODUCTION**

The Oracle database system's behavior is governed, in part, by its numerous Initialization Parameters, which define many internal database settings. Oradjuster is concerned with two small groups of these parameters. The first group regulates the memory usage of **oracle.exe**, and the second group controls the number of client programs that can be connected simultaneously to the database.

Although Oradjuster is not mandatory, it is very helpful. For many investigators, it is ideal to run Oradjuster immediately following the AD Oracle install by clicking the *Optimize the Database* button on the Database installation autorun menu. Later on, Oradjuster can be invoked again (one or more times) in order to fluctuate database

memory usage and derive even greater FTK performance gains throughout the several phases of an investigation.

## THE FIRST INVOCATION

When Oradjuster is invoked for the first time, it does the following:

1. Detect AD Oracle
2. Query Windows to discover the size of RAM
3. If necessary, prompt for the database's administrative password
4. Display the current values of the parameters of interest
5. Compute new values (based on the size of RAM) and modify the parameters with them
6. Shut down and restart the database
7. Display the updated parameter values
8. Record the new values in a Windows Registry key

Some of these steps will be treated in greater detail in what follows.

**Note:** When Oradjuster is invoked from the install autorun menu, it does not linger on screen. It disappears as soon as it has completed successfully, which is done in deference to those who may not take an interest in its esoteric display information.

Oradjuster's first invocation brings great improvement to FTK's performance, and many investigators may find this satisfactory. However, as mentioned previously, subsequent use of Oradjuster can yield additional performance improvements.

## SUBSEQUENT INVOCATIONS

The use case scenarios described in this section illustrate how to employ Oradjuster to greatest effect in the two FTK deployment configurations known as One-Box and Two-Box.

**Note:** Some of the instructions below describe the invocation of Oradjuster from the command prompt. Working from the command prompt may be a foreign experience for many, but any time/effort spent becoming familiar with the command prompt and command line programs is worthwhile because it facilitates advanced use of Oradjuster, and it opens a door to the large number of valuable and intriguing command line programs available (serving many diverse purposes, including digital forensics).

## ONE-BOX FTK DEPLOYMENT

Oradjuster's default behavior is to assume that FTK and AD Oracle are installed on the same computer. The settings it applies on its first run therefore strike a balance between the memory needs of FTK, AD Oracle, and the operating system. Additional performance gains can be won by reducing **oracle.exe** memory consumption during FTK's evidence processing, and then increasing **oracle.exe**'s memory consumption during investigative analysis after automatic processing has completed. To accomplish this fluctuating of **oracle.exe** memory usage, do the following:

1. After creating a case, but before adding and processing evidence, launch Oradjuster from the Case Manager's Tools menu.
2. Oradjuster will display its normal output, and then prompt the user to make a temporary change to **SGA\_TARGET** (one of the Oracle database parameters having direct impact on memory consumption). The value for **SGA\_TARGET** is specified as a percentage of the size of physical memory, and the allowable range is typically between 10% and 50%. Enter a percentage in the lower half of the allowed range.
3. Add and process the case's evidence.
4. After processing is complete, launch Oradjuster again from the Case Manager's *Tools* menu.
5. Modify **SGA\_TARGET** to a percentage in the upper half of the allowed range.
6. Complete the investigation of the case without modifying **SGA\_TARGET** again unless more evidence is added and processed.

As the reader may surmise, some trial-and-error experimenting is required to find the most optimal percentages. For example, it may be desirable to set **SGA\_TARGET** to the maximum allowable percentage in Step 5, rather than just some percentage in the upper half of the range, so that FTK's case window is most responsive. Also, it may be good to reduce **SGA\_TARGET** during Live searching (in spite of Step 6) as Live searching is similar in nature to evidence processing.

## TWO-BOX FTK DEPLOYMENT

When FTK is installed on computer A, and AD Oracle is installed on computer B, **oracle.exe** should be even more aggressive in consuming memory on computer B since it does not need to share memory resources with FTK. The following procedure should be conducted.

To begin, log in to computer B.

**Note:** If Oradjuster has been run on this computer before (as part of AD Oracle install and setup), then its Registry key must be deleted before proceeding. Select Start Menu > *Run*.

Type “regedit” in the Run prompt and press Enter. Within the Registry Editor dialog, navigate to and delete the following key:

HKEY\_LOCAL\_MACHINE\Software\AccessData\Shared\Version Manager\  
sds\oradjuster

**Important:** Do not delete or modify any other Registry keys or your system may become unstable.

Open the command prompt (select *Start Menu > All Programs > Accessories > Command Prompt*). Then issue the following commands (press the Enter key after each one):

**TABLE 1-1**

Command	Explanation
C:\> cd “Program Files\AccessData\Oracle\Oradjuster”	Move to the directory containing Oradjuster.exe. On a 64-bit version of Windows, the directory path should be “Program Files(x86)\AccessData\Oracle\Oradjuster”.
C:\[path]> Oradjuster.exe -mem remoteworker	Assign parameter values appropriate for a dedicated AD Oracle database.

As with Step 6 in section *The First Invocation*, and the database will be restarted. Some of the Oracle parameters managed by Oradjuster cannot be modified “on the fly”, so the database must be restarted in order for their changes to take effect. Therefore, when invoking Oradjuster from the command prompt, first close FTK (by closing all case windows and the case management window).

## TUNING FOR LARGE MEMORY SYSTEMS

When AD Oracle resides on a computer with a 64-bit Windows operating system, and with a large quantity of RAM (from 8 GB to 128 GB, or higher), additional considerations are in order. As was hinted in section *One-Box FTK Deployment*, Oradjuster’s first run assigns **oracle.exe**’s maximum memory consumption to roughly ½ the size of RAM. (That is why the upper limit for **SGA\_TARGET** is typically 50%.) Instead of sharing memory proportionally between AD Oracle and the operating system (and possibly FTK), Oradjuster can be used to give **oracle.exe** the lion’s share of memory, which would not be safe on a computer with a lesser quantity of RAM. This is best accomplished by editing Oradjuster’s key in the Registry and then running Oradjuster again, which causes Oradjuster to apply the new, manually-entered values in the Registry key to AD Oracle.

Consider an investigative computer with 64 GB of RAM that hosts AD Oracle and FTK. Suppose that the investigator ran Oradjuster in conjunction with the AD Oracle install, and has since conducted several large cases (containing millions of discovered items

each) in FTK. The investigator is generally content with the FTK case window's responsiveness in loading and sorting its File List pane, but wonders if that responsiveness could be improved. So, she prepares to edit the `SGA_MAX_SIZE` and `SGA_TARGET` values in the Oradjuster key in the Registry. When she opens Registry Editor and first navigates to the key, she sees that current values read:

**TABLE 1-2 Example of Oradjuster Settings**

Name	Type	Data
...	...	...
sga_max_size	REG_SZ	37795712204
sga-target	REG_SZ	13743895347
...	...	...

These values represent quantities expressed in Bytes, and therefore the investigator can see that Oradjuster has set `SGA_MAX_SIZE` to about 37 GB, and `SGA_TARGET` value of roughly 13 GB. She knows that she can temporarily alter the value of `SGA_TARGET` using the technique shown in *One-Box FTK Deployment*, but she can only increase it to the upper limit imposed by `SGA_MAX_SIZE`. So, she decides to make the following edits:

**TABLE 1-3 Example of User-Modified Oradjuster Settings**

Name	Type	Data
...	...	...
sga_max_size	REG_SZ	48795712204
sga-target	REG_SZ	32743895347
...	...	...

By modifying only the first two digits of Data field for each value, the investigator has paved the way for Oradjuster to make the desired change to AD Oracle. (If she had wanted, the investigator could have edited the Data field to contain a number that would be easier to read, such as “48000000000”, but the net effect would be the same. And, the smaller the edit, the less chance of loosing a digit or inserting an extra one, both of which may require a troubleshooting effort to repair.) As soon as Oradjuster is again invoked, the new upper limit for `oracle.exe` memory usage will be approximately 48 GB (a jump from about 1/2 to about 3/4 of RAM), and `SGA_TARGET` will be set to about 1/2 of RAM by default.

The investigator closes FTK (knowing that her edit of `SGA_MAX_SIZE` in the Registry will cause Oradjuster to restart AD Oracle) and runs Oradjuster again. (In this context, she can do so either by invoking it from the command prompt, or by launching it with

a double-click using the mouse.) When Oradjuster completes its assignment changes, and prompts the investigator to make a temporary change to `SGA_TARGET` if desired, she pauses to review the before and after values in the Oradjuster output to confirm that the changes to `SGA_MAX_SIZE` and `SGA_TARGET` are correct.

**Note:** When Oradjuster assigns a new value to `SGA_MAX_SIZE`, `oracle.exe` will modify it rounding it up the nearest multiple of 16 MB. Therefore, when inspecting Oradjuster output, remember to confirm that the first (or left-most) digits of `SGA_MAX_SIZE` are correct. Do not be alarmed if trailing digits have been altered.

Finally, the investigator creates several more large FTK cases with her new settings. She observes that the FTK case window is in fact more responsive and she pays attention to evidence processing times to see whether or not `oracle.exe`'s increased claim on system memory appears to slow down evidence processing..

In conclusion, and although the vast majority of tuning needs have been addressed by the preceding information, additional explanation will allow a curious investigator to go even further in using Oradjuster. First, the list of supported command line arguments can be displayed with the command:

```
C:\[path]> Oradjuster.exe -help
```

Second, the following table provides a listing of the values Oradjuster records in its Registry key.

**TABLE 1-4 Oradjuster Values Found in its Registry Key**

Value Name	Provokes DB Restart	Type
<code>_pga_max_size</code>	NO	Memory Usage
<code>_smm_max_size</code>	NO	Memory Usage
<code>commit_write</code>	NO	Memory Usage
<code>open_cursors</code>	NO	Memory Usage
<code>pga_aggregate_target</code>	NO	Memory Usage
<code>processes</code>	YES	Number of Concurrent Connections
<code>session_cached_cursors</code>	YES	Memory Usage
<code>sessions</code>	YES	Number of Concurrent Connections
<code>sga_max_size</code>	YES	Memory Usage
<code>sga_target</code>	NO	Memory Usage

**TABLE 1-4 Oradjuster Values Found in its Registry Key**

---

<b>Value Name</b>	<b>Provokes DB Restart</b>	<b>Type</b>
Transactions	YES	Number of Concurrent Connections
VERSION	N/A	Oradjuster Version Information — Do not edit

