



**Administrator Workplace  
Administration Guide**

# Contents

<b>CONTENTS</b> .....	<b>2</b>
<b>1 INTRODUCTION</b> .....	<b>3</b>
1.1 REQUIREMENTS .....	3
<b>2 INSTALLATION</b> .....	<b>4</b>
2.1 USER INTERFACE .....	4
2.2 ADMINISTRATOR WORKPLACE MANUAL .....	5
2.2.1 <i>Sessions management</i> .....	6
2.2.2 <i>Creating and restoring backup copies of database</i> .....	6
2.2.3 <i>User management</i> .....	7
2.2.4 <i>Services management</i> .....	7
2.2.5 <i>Biometrics server settings</i> .....	8
2.2.6 <i>Communication server settings</i> .....	9
2.2.7 <i>Logs viewing</i> .....	10
<b>3 CONTACT US</b> .....	<b>12</b>

# 1 INTRODUCTION

This user guide gives an introduction to the *Administrator Workplace* application.

It explains the use cases of the *Administrator Workplace* application and environment settings. The *Administrator Workplace* application provides all needed functionality for servicing and management of Biometric and Communication server applications.

## 1.1 Requirements

*Administrator Workplace* is a Windows-based application.

The recommended system requirements are as follows:

- Windows® 7 Service Pack 1;
- 1024X768 minimum display resolution;
- Intel® Core 2 Duo® E8500 or AMD® equivalent;
- 2 GB RAM or higher;
- .NET Framework 3.5 Service Pack 1;
- TCP/IPv4 support.

The minimum system requirements:

- Windows® XP Service Pack 3;
- 1024X768 minimum display resolution;
- Intel® Pentium® IV 2.8 GHz or AMD® equivalent;
- 512 Mb RAM;
- .NET Framework 3.5 Service Pack 1;
- TCP/IPv4 support.

## 2 INSTALLATION

The *Administrator Workplace* application is distributed as an executable file with a built-in installer. You need to follow the installation wizard instructions.

### 2.1 User Interface

After starting the *Administrator Workplace* application you will be requested [figure 1.1] to enter authentication data: a login and a password. Usually changes in connection settings are required [figure 1.2]. It is vital to use the *Administrator Workplace* application only at the computer of the responsible administrator. Usage of other methods (embedded tools of MS Windows, HASP etc.) of access restrictions is mandatory.

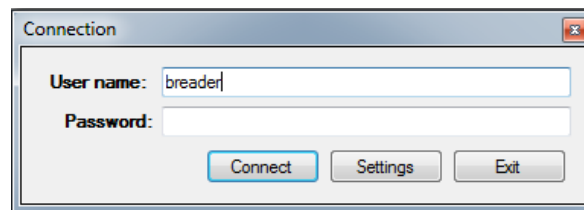


Figure 1.1: Authentication dialog

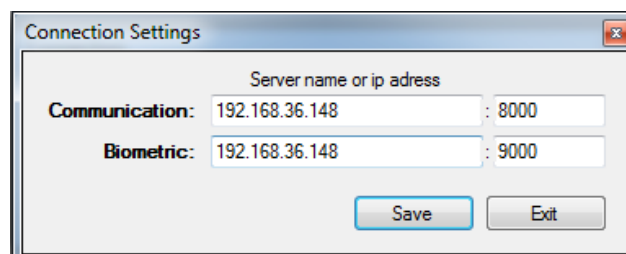


Figure 1.2: Connection settings

In case of successful authorization you will see the main window [figure 1.3] of the *Administrator Workplace* application. It consists of several areas. At the top of the window there is a menu of interoperability with the application. In center of the window there is an area for operating with

various tools. At the bottom of the window there is an information area.

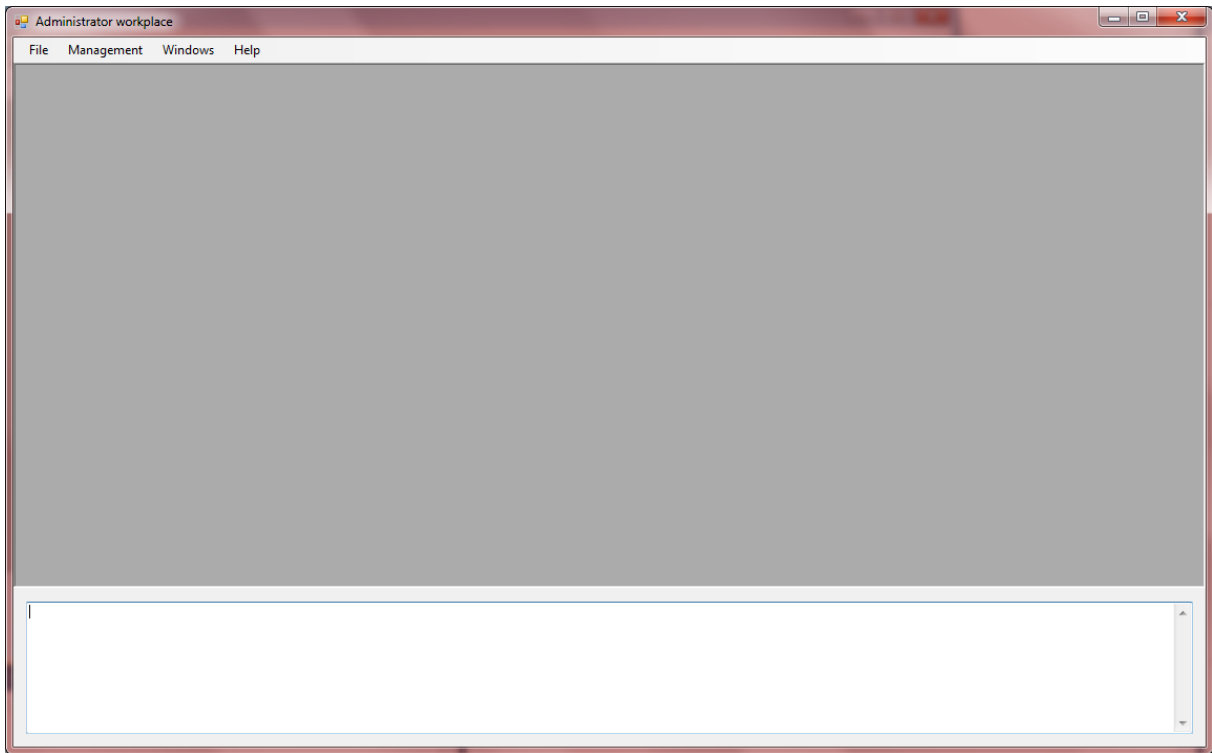


Figure 1.3: Main window

## 2.2 Administrator Workplace Manual

All available tools are run from the *Management* menu. It includes:

- *Sessions* – a list of sessions with possibility to stop any session;
- *Backup* – creation of database backup copy;
- *Users* – management of users;
- *Services* – management of *Biometric* and *Communication* services;
- *Logs* – viewing of logs;
- *Settings* – changing of *Biometric* and *Communication* services options;
- *Investigator Log* - viewing of investigative logs.

## 2.2.1 Sessions management

Sessions tool [figure 1.4] provides a table with all open connections to the SQL server and a button *Kill sessions*. In order to close any session you need to select the respective record in the table and push the *Kill sessions* button.

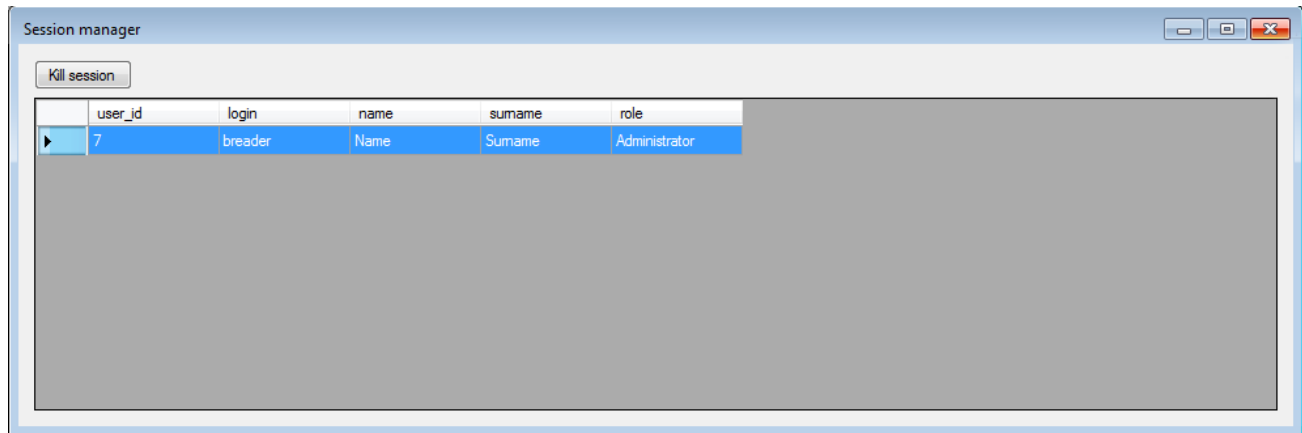


Figure 1.4: Sessions tool window

## 2.2.2 Creating and restoring backup copies of database

Backup tool [figure 1.5] allow to choose a path for storing a backup copy of the database, backup the database as well as restore the database from the previously made copies.

We also suggest using third party backup applications or utilities in order to increase the safety of data.

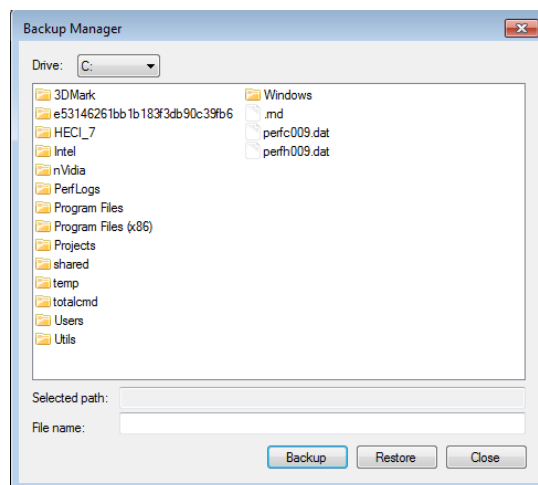


Figure 1.5: Backup tool window

### 2.2.3 User management

User management tool [figure 1.6] window includes a list of users and the detailed information window. Administrator can create, manage and delete users, using the appropriate buttons. Please note that for the security reasons you have to set reliable passwords and do not grant higher rights than it is needed to users.

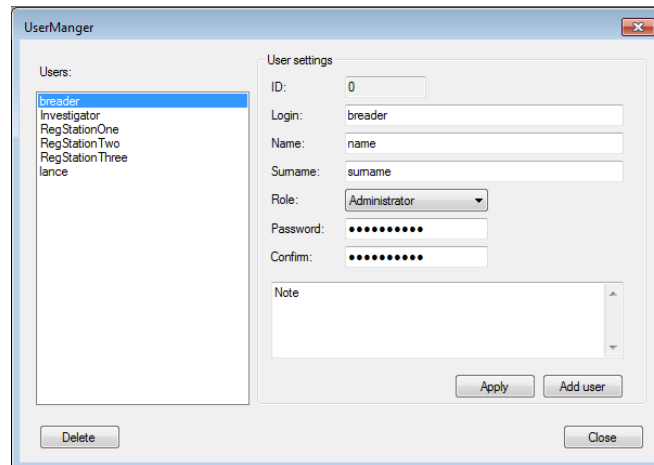


Figure 1.6: User management tool window

### 2.2.4 Services management

To manage services of both biometric and communication servers user must have administrative rights. Credentials dialog [figure 1.7] allows Administrator to set user name and password of administrative account of specific server – select the server from the server list, type User name and password and click the *Save* button. Software will use these user name and password to configure server services

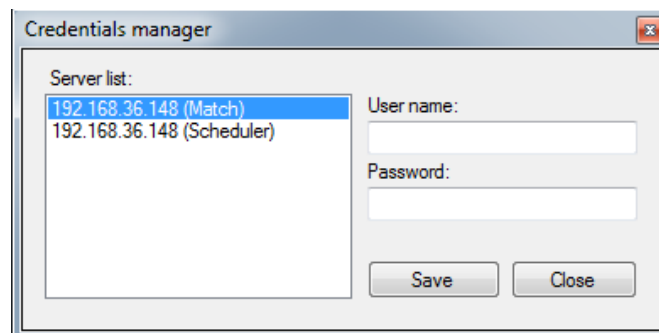


Figure 1.7: Credentials management dialog

Services tool [figure 1.8] is dialog for management servers' services. There is information regarding current status of each server and buttons for start, stop and restart commands.

**WARNING!** It is vital to check the status of the server side applications and avoid unnecessary stops of services.

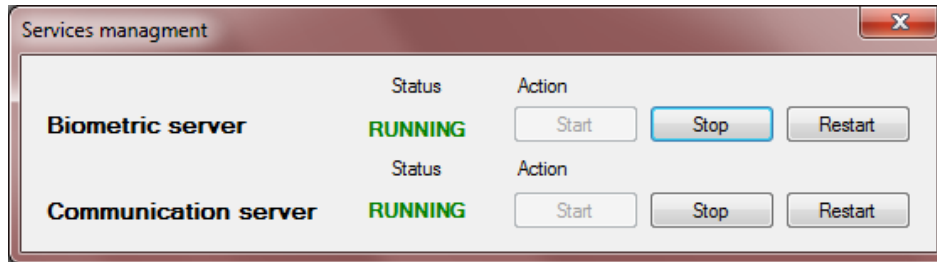


Figure 1.8: Services tool window

### 2.2.5 Biometrics server settings

Settings dialog [figure 1.9] allows Administrator to configure biometric server. The following parameters can be configured:

- *Listen interface* – IP-address and port of biometric server. The port should be opened in firewall for incoming connections;
- *Log directory* – directory path to store biometric server log file;
- *Log rotation size* – maximal file size in kilobytes when to rewrite log file;
- *Log verbosity level* – level of log detailing:
  1. *None* – do not write log file,
  2. *Error* – write errors only,
  3. *Warning* – write errors and warnings,
  4. *Debug* – write errors, warnings and debug information.



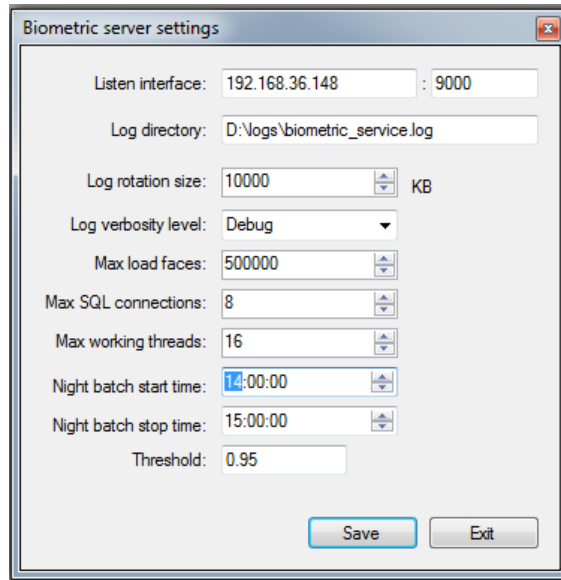


Figure 1.9: Biometric server settings dialog

- *Max loaded faces* – maximum of loaded faces by biometric server (if set to zero (0), then all faces will be loaded);
- *Max SQL connections* – maximum of parallel SQL connections to the biometric server;
- *Max working threads* – maximum of working threads for query processing on the biometric server;
- *Night batch start time* – time when night batch starts;
- *Night batch stop time* – time when night batch stops (if some tasks have incomplete status, they are terminated);
- *Threshold* – biometric similarity threshold. This parameter sets threshold when two persons treats as a similar person.

## 2.2.6 Communication server settings

Settings dialog [figure 1.10] allows Administrator to configure communication server. The following parameters can be configured:

- *Listen interface* – IP-address and port of communication server. The port should be opened in firewall for incoming connections;

- *Log directory* – directory path to store communication server log file;
- *Log rotation size* – maximal file size in kilobytes when to rewrite log file;
- *Log verbosity level* – level of log detailing:
  1. *None* – do not write log file,
  2. *Error* – write errors only,
  3. *Warning* – write errors and warnings,
  4. *Debug* – write errors, warnings and debug information.

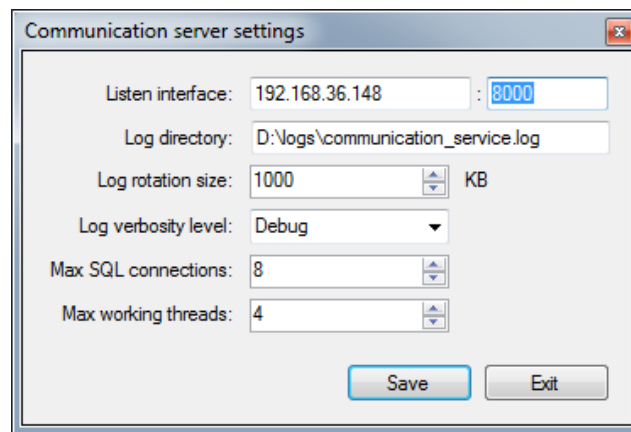


Figure 1.10: Biometric server settings dialog

- *Max SQL connections* – maximum of parallel SQL connections to the communication server;
- *Max working threads* – maximum of working threads for query processing on the communication server.

### 2.2.7 Logs viewing

Logs tool [figure 1.11] gives an opportunity to look through all events and apply a needed filter. It is possible to choose the user ID and indicate time slots.

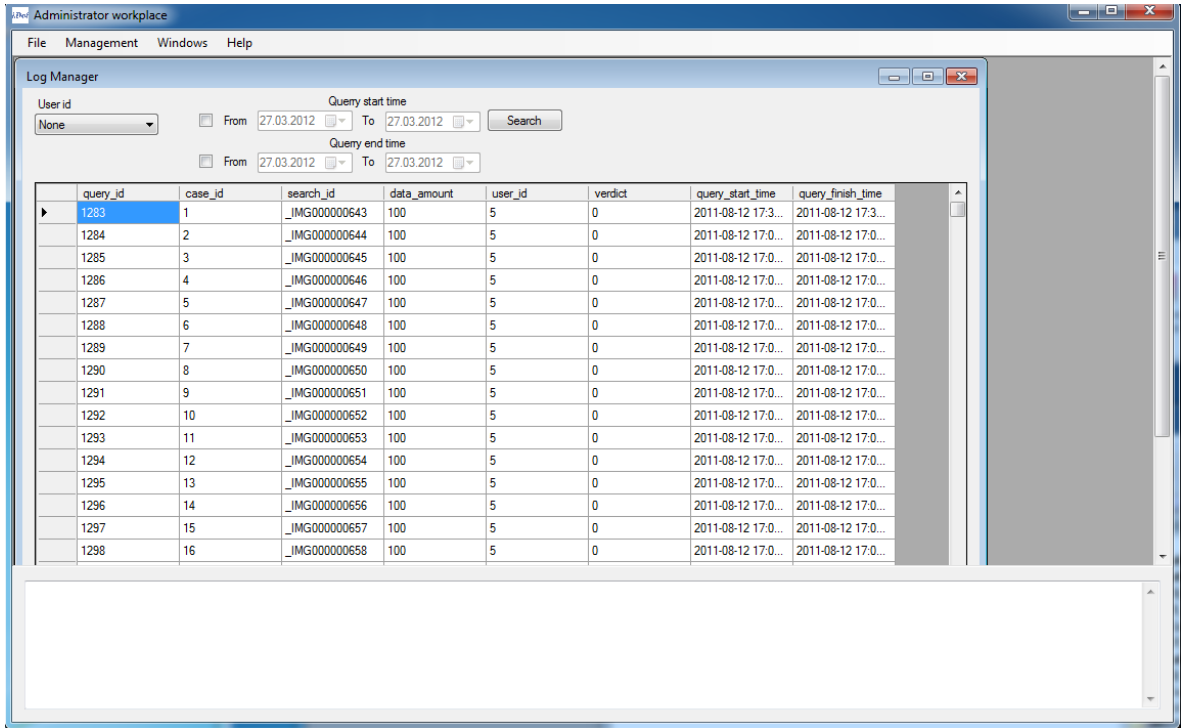


Figure 1.11: Logs tool window

Administrator can also view all actions of an investigator on the selected case [figure 1.12]

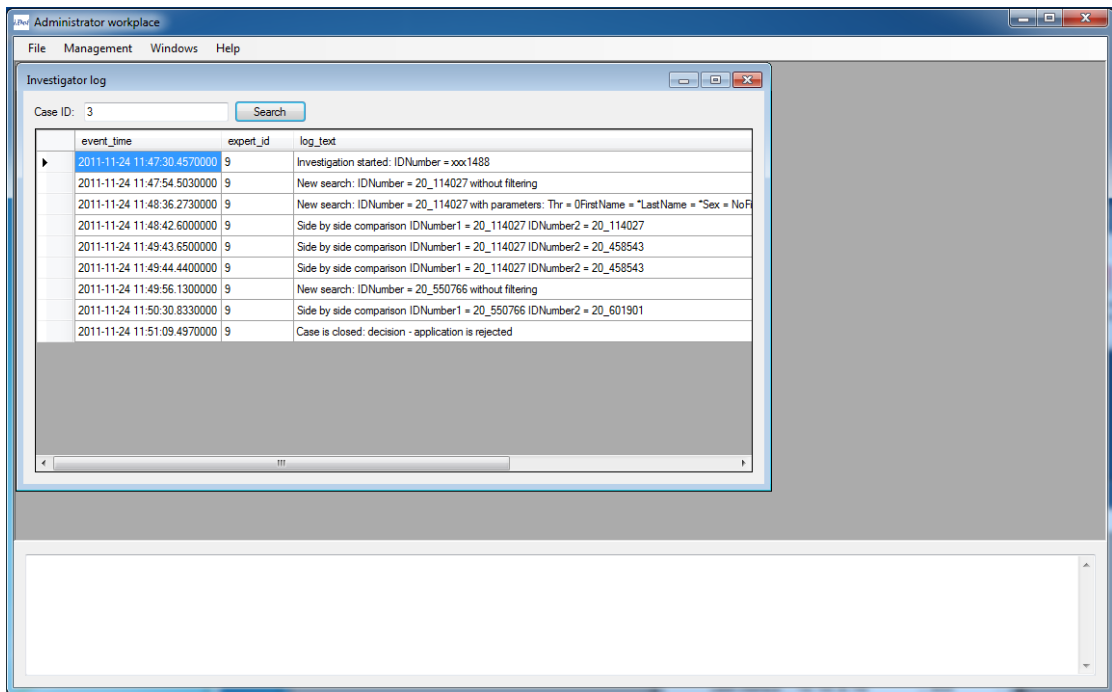


Figure 1.12: Investigator logs tool window

### 3 CONTACT US



#### Headquarters

**Institute of Digital and Optical Technologies B. V.**

**Postal address:** De Lairesestraat 160-C, 1075 HM  
Amsterdam, The Netherlands

**Fax:** +31.20-8908634

**E-mail:** [bizdev@idotbio.com](mailto:bizdev@idotbio.com)  
[bizdev@idotbv.nl](mailto:bizdev@idotbv.nl)

**Web:** [www.idotbio.com](http://www.idotbio.com)  
[www.idotbv.nl](http://www.idotbv.nl)

Copyright © 2013 Institute of Digital and Optical Technologies B. V. All rights reserved.

This guide is for informational purposes only. No warranties, express, implied or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Institute of Digital and Optical Technologies B. V.