Welcome to Omniquad Desktop Surveillance

For latest information and program updates, visit our Home Page at
http://www.omniquad.com

What Is Your Computer Up To When You Are Not There?

Omniquad Desktop Surveillance offers a unique approach to the problem of access control, prevention of, or investigation into, use/misuse of computer equipment and software. Instead of merely obstructing the user's actions, one of the oldest prevention methods known - the prospect of being watched and 'found out' - is applied.

The program is the software equivalent of a surveillance camera and works by recording desktop activity. Yet it may operate in two modes; either by displaying warning signs in order to discourage misuse, or by secretly monitoring activity. While the application can store days of recordings, the settings can be tailored virtually for any situation. For example, recording can be activated at certain chosen times only, when running specified applications or on log-on to the Internet.

This application is the only tool available to address not only the issues of web browsing but also newsgroups and IRC at the same time. The program recording can be activated as soon as you visit certain WWW sites or specific IRC channels. Desktop Surveillance can also be remotely controlled, either via local network or the Internet, and in both cases it is possible to remotely observe activity on the local desktop in real time. The program can be applied in a manifold of situations - for example to discourage employees in your office from visiting specified WWW sites or performing certain tasks, or maybe to secretly find out what your PC is being used for in your absence. Unlimited number of users can be added, each with an individual surveillance profile.

User Profiles

Desktop Surveillance Profiles allow the system administrator to configure a unique surveillance set-up for each user on the local computer or network.   When user logs-on, Desktop Surveillance agent will try to load a profile with filename corresponding to the user name (for example when user JSMITH logs-on, the agent will try to load profile named JSMITH.CFG).   If the requested profile is not found, default profile will be loaded (DEFAULT.CFG).   On a network, workstations can be configured to load profiles from one location, so the system administrator needs to configure them only once.

Adding User Profiles

To add User Profiles to the list, click the **Add User** button in the Profiles section and enter the user name in the text box that appears.   The user name is the login name.

Editing User Profiles

- Select the user profile that you want to edit.
- Click the **Edit** button.
- Make changes to the various sections and click **OK**.

Removing User Profiles

Select the user profile that you want to remove and click the **Remove** button.

General

Enable Desktop Surveillance: If this setting is disabled, Desktop Surveillance will automatically auto-terminate and free the computer memory. This setting would be normally disabled in a profile for a user that will be not under surveillance.

Example 1:
On a computer with user names TOM, DICK, HARRY and SUSAN, Tom's actions should be recorded, other users are not under surveillance. Two profiles should be present:

Profile TOM.CFG should have option 'Enable Desktop Surveillance' set ON
Profile DEFAULT.CFG should have option 'Enable Desktop Surveillance' set OFF

Example 2:
On a computer with user names TOM, DICK, HARRY and SUSAN, Tom's actions should not be recorded, everybody else is under surveillance

Two profiles should be present:
Profile TOM.CFG should have option 'Enable Desktop Surveillance' set OFF
Profile DEFAULT.CFG should have option 'Enable Desktop Surveillance' set ON

If a new user logs-on, profile DEFAULT.CFG will be loaded in each case

Register Task Name: This is what the user can see in the task list. It is recommended that meaningless name is entered, such a 'ODS' etc, so that it is not obvious for the user that Desktop Surveillance is running.

Disable Task Switching: Choosing this option makes it impossible for the user to terminate any program from the task list or even determine if it is running.

Allow termination from Task Manager: Enables user to terminate the program from the Task Manager. If this option is disabled, Desktop Surveillance will initiate Windows shut down if user tries to terminate it from the task list.

Enable Remote Surveillance: Allows for the workstation running Desktop Surveillance to be monitored from a remote computer. Recording can be also activated/deactivated remotely. You should consider the associated security risks before enabling this option. See the Network Surveillance for more information on how to use remote surveillance.

Listen on Port: Specifies the port to use in the remote surveillance operations (default 1005) - the port settings should be the same on all the computers on the network.

Enable Debug Window: Displays current status of Desktop Surveillance - this option is included to aid testing Desktop Surveillance.

Activity Log

Enable Activity Log to periodically save memory contents to a file. The Activity Log provides alternative surveillance solution to the visual recordings. The reports can be saved to a text file or ODBC data source.

NOTE: Enabling ODBC logging will increase memory usage as database drivers will be loaded.

Desktop Surveillance database logging

Requirments: ODBC version 3.0 or higher

Instead of text file, Desktop Surveillance can log user activities to a database via ODBC. To use activity logging, you can use the supplied template ODSLOG.MDB and configure it as a new data source, or recreate the necessary table and fields on proprietary database system

Step-by-step instructions: configuring database logging with supplied template:

ensure that ODBC version 3.0 or higher is installed
open Control Panel 32-bit ODBC applet
select system DSN and click on ‘ADD’ button
select Microsoft Access Driver and on the ‘Finish’ button
enter a new Data Source Name, such as ‘ODSLOG’
Click on the ‘Select’ button and find file ODSLOG.MDB in the installation directory
Close Control Panel
Specify the new Data Source Name in Desktop Surveillance activity log section

Step-by-step instructions: configuring database logging with existing ODBC data source

- Create new table with name ‘ODSLOG’ in existing data source, adding the following fields:

UserName char(10)
TimeStart DateTime DateTime or char(15)
TimeEnd DateTime DateTime or char(15)
ActivityDescription char(30)

- Specify the new Data Source Name in Desktop Surveillance activity log section

Triggers

This section lets you configure when Desktop Surveillance will start and stop recording activity. Recording will start if **any** of the conditions is true and terminate when the condition is false.

Always: Selecting this option means that recording will start immediately when Surveillance Agent is loaded. Enable this setting if you want to keep recording everything that happens from the moment the computer logs on to Windows. Enabling this option automatically overrides all other settings in this section.

On Time: This will activate recording at time specified. Use HH:MM format (and the program will keep recording until you terminate the Windows session).

Trigger List: When Desktop Surveillance Agent is running in the background, it will periodically check all the applications and processes currently running. If any of the programs loaded matches entry on your application trigger list, the recording will be activated immediately. If user exits the application, the recording will stop.

You don't have to enter the exact name of the application you want to add to the trigger list, all you have to enter is a part of the application's name (as it would appear in the application's window caption or in Windows Task List). As some programs do not show any windows and are not on the task list, you may click on the 'List Active' button to see a list of all active processes.

For example, if you want to record only when user is using the Notepad program, you can add text **notepa** to the Trigger List (the last letter 'd' is omitted intentionally to show you exactly what the program does). When the Desktop Surveillance Agent loads, it will periodically check all the running applications. Because no applications in the process list have text **notepa,** the entry will be not matched and nothing will happen. However, when the user starts Notepad, there will be a new item in the Windows task list, for example **Untitled Notepad.** When the Agent makes next task list comparison, it will match **notepa** with **Untitled Notepad** and trigger recording. The same applies to entering parts of a document name into the trigger list. You could enter document name keywords, such as **prohibit**. When the user browsing the Internet, he or she would visit the following several sites, but in none of them the specified word would appear. As the user is visiting different WWW sites (say using application Internet Browser), the task windows would keep changing:

Internet Browser (http://www.worldhistory.com)
Internet Browser (http://www.omniquad.com)
Internet Browser (http://www.downloadsoftware.com/newdownloads)

None of the tasks contain word **prohibit,** so nothing will happen. If the user visits for example site Internet Browser (http://www.prohibitedrinks.com, the Surveillance Agent would start recording because the window task name contains the word **prohibit**

If you want to record everything when the Internet Browser application is running, regardless of sites visited, you enter the word **Internet** or **Browser** into the trigger list.

The Trigger list is a very useful feature, it monitors not only the applications that appear in the Task List but also all running processes, thus giving you more flexibility in specifying the recording times.

Accuracy

You can set Desktop Surveillance to take screen snapshots at set intervals.   Shorter intervals will record with more accuracy, but will take up more system and disk resources. You can also choose the colour depth with which the recordings will be made: Black & White, High Colour or 16 colours.

It is also possible to set the program to skip identical frames in order to save recording storage space.

Working Modes

Desktop Surveillance can operate in two modes:

Secret Surveillance: The user is not aware that everything he or she does is or can be recorded.   The situation can be compared to a hidden security surveillance camera.

Surveillance with Warnings (Prevention): The user is warned that any activity can be recorded.   You can use this mode to discourage the user from doing something he or she is not supposed to do.

To enable the Prevention mode, apply any of the settings below:

Warning: A text message appears when the Surveillance Agent is loaded into the memory to inform the user that any activity may be recorded.

Show Animated Icon: Enabling this option will show a 'moving eye' indicator in the task area, so that the user is kept aware of the monitoring process.

Recording to Disk

Save Recordings to Disk: This section lets you decide if you want to save the recordings to a disk.   This is useful particularly if the system administrator wants to have the program running in order to inspect various desktop activities over a network in real time but do not want to store these recordings. This section will also let you decide where to save the recorded folders.

Create New Subfolder For Each User: Use this option to aid management of surveillance recordings (a new subfolder will be created for each user, the recording sessions will indicate not only the initial recording time but also the computer name.   This option allows the network administrator to configure all the workstations on the network to save recordings to the same root folder on the network server.

Reserve Disk Space: You can decide how much disk space to reserve for each user profile. Once the set limit is reached, the recording will stop.

E-mail

The recordings can be automatically E-mailed to a specified E-mail address.   To use this option, check the box ‘Enable e-mail forwarding’ and specify an E-mail address.

FTP

Desktop Surveillance can save the recordings on a remote FTP server.   The benefit of using a remote FTP server is that the recordings cannot be removed after they are saved.   (The user can delete recording files when the Recording To Disk option is used.)   The recordings can also be inspected from anywhere - without a need to access the original workstation where they were made.

For more information on obtaining FTP space on an Internet host, check URL http://www.omniquad.com/ftpspace

TCP/IP

If the E-mail option is to be used, it is necessary to specify what kind of TCP connection the computer(s) has (have).

SMTP and FTP recordings are buffered and then sent in one batch to the servers. The buffer setting indicates the time period (in minutes) which should elapse before each new batch is sent. If any recordings where not sent to the server during the current session, they will be processed in the next one.

On a shared-network installation of Desktop Surveillance, you can route all the traffic though one workstation.   See the help file for more information on the shared network installation

When routing the surveillance recordings via the Internet. you should configure high interval settings to minimise the amount of traffic, otherwise you may risk jamming your own network connection (or e-mail account) and other Internet hosts.   **See the help file for more information on this topic**

Playback

To playback any recording, simply select the **Playback** tab, browse to the folder which corresponds to the session name (user profile name) and click on the **View Session** button. Ensure that you double-click on the folder, so that you will see opened folder icon.   Use the on-screen buttons to navigate through the playback.

Network

Remote Surveillance requires your computer to be a part of a network running TCP protocol, (it is / can be running on Intranet, Internet, LAN or small workgroup). When entering the remote workstation's name, you can specify either the workstation's computer name or it's IP address.

To find out the computer name, open Network settings in Control Panel and click on the **Identification** tab. The workstation's IP address can be obtained from the TCP protocol settings in the **Configuration** tab.

To ensure that your network is ready for remote surveillance sessions, try to PING other workstations, for example:

```
ping 192.161.0.7
ping johnycomputer
```

If you are getting no results, you should resolve TCP protocol problems before continuing

Enabling Remote Surveillance option enables the following functions:

- **Remote Activation**

You can activate recording on a remote workstation. This will override any recording settings on the workstation in question.

- **Remote Deactivation**

You can deactivate recording on a remote workstation. This also overrides any surveillance settings on that workstation

- **View**

You can monitor activity on the remote workstation in real time

Any workstation you want monitor needs to have Desktop Surveillance active and the Remote Surveillance option has to be enabled in the active user profile. All the workstation on the net work should be configured to use the same port.

Before you enable the Remote Surveillance option, you should consider associated security risks.

Network Administration Notes

Follow the directions below to install Desktop Surveillance on a network. You can configure these commands to start within a batch file, automatically executed on each workstation which is logged on to the local network. The automatic installation part should be executed separately (the workstations will need to be rebooted before continuing with the next step), other commands can then be executed together in one batch file.

Automatic Installation

To automatically install Desktop Surveillance on end workstation, execute this command while in the application's setup folder:

```
setup.exe -s odsinst.log
```

The application will install itself into folder 'c:\program files\ods' without any user interaction

Shared start-up location for each workstation

Shared network installation allows the system administrator to manage the whole surveillance network from a central location. When a user logs on any workstation in the network, his surveillance profile will be executed on that workstation.

To create a shared installation:

- Create a shared folder on the server (or other peer-to-peer workstation which is always turned on).
- Copy the following files to the new shared folder:

```
spn.exe
ods.dat
ods.lic
default.cfg
```

When a new user profile is created, it will be saved to the same folder where the application was launched from, therefore Desktop Surveillance should always be started from the shared location.

- Adjust the start-up path for Desktop Surveillance module on each workstation. By default, the application is always initiated from registry key:

```
hkey_local_machine\software\microsoft\windows\currentversion\run\ods25
```

To set a start-up location for Desktop Surveillance, execute the *setstartuppath* module, with the new path passed as a command line parameter, for example:

```
setstartuppath.exe \\ntserver\share_c\spn.exe -r
```

When started with the -r switch, the program will activate itself. If the switch is missing, it will load the user interface (as when loaded from the start menu) on each workstation. It is therefore important that the -r switch is included.

License File

The license number should be entered as soon as you launch any surveillance operations. The license number is stored in file ods.lic, which must always be present in the program directory. If the number of workstations on the surveillance network exceeds the one specified in the license, delete the license file and re-enter the license number.

Removing Program Folder

The program folder can safely be removed if Desktop Surveillance always will be loaded from network path.   To remove the program folder, execute:

```
removeredundant.exe
```

Removing Shortcuts

To remove the program shortcut from the current user’s start menu, execute:

```
removeshortcut.exe
```

Sample Run

Follow these step-by-step instructions to create and replay a simple recording.

- Select the default user profile in the main window and click the **Edit** button. The default profile has sample options already set.

- Select the various tabs:

    - **General**: Tick the option ‘Enable Desktop Surveillance’ and ‘Allow user to terminate Desktop Surveillance from the task list’.

    - **Triggers:** Tick option ‘Always’. Desktop Surveillance will begin recording as soon as the user logs-on.

    - **Accuracy:** Set the snap interval to 0 minutes 5 seconds.

    - **Recording to Disk:** Enable ‘Save Recordings to a Disk’ and select a folder where you wish to save the recordings. (E.g. c:\temp)

    - Click **OK**.

- Exit from the program and restart the computer. Desktop Surveillance memory-resident agent will load the new profile at start-up.

- When Windows loads again, there will be a warning message telling you that Desktop Surveillance has been activated. There will be another small window showing you the status (this feature has been enabled for test purposes only). Within few seconds, the window’s text should be ‘recording active’.

- For the next few minutes, work with a few different applications, edit some documents or browse the Internet
  Now, use Windows explorer to go back to the folder where you specified to save the recordings. A new sub-folder should be there, and its name would be a combination of date and time when the recording session has started. If you check the contents of the folder, you will see that every few seconds there is a new file appearing (these files are actual screen shots saved at regular intervals).

- Press CTRL-ALT_DEL , end task ‘ODS’.

- Open Desktop Surveillance from the Start Menu. In the **Playback** tab, select the folder with a session name and click the **View Session** button (make sure that you double-click on the folder, so that you will see the opened icon).

- Now you can replay the entire recording. Instead of your real desktop, you will see what was the desktop’s content at the time of the recording.

Points to Note

Maximising Workstation Performance

If there is no need for a continuous surveillance operation, the users' profiles should be disabled. In this way, no system resources are consumed. (Please refer to the 'Program Options' topics for more about profiles.) When there is a large number of users, the surveillance administration should start with just one disabled (DEFAULT) profile. New profiles for users that are supposed to be under surveillance can then be added when necessary. The downside of this approach is that surveillance operations for a particular user cannot be initiated until he or she logs on next time (after the system manager has enabled his or her profile). If all users are supposed to be under surveillance from day one, the system can still run with just one profile (DEAFULT), which in this case should be enabled. When each user logs on, Desktop Surveillance tries to load the current user's individual surveillance profile. If individual profiles cannot be found, the DEFAULT profile will be loaded.

If remote real-time surveillance of any workstation is a necessity, Desktop Surveillance should be always enabled, in the DEFAULT and in the individual user profiles. In this way the program will stay loaded, and ready for surveillance operations.

NOTE: Enabling ODBC logging will increase memory usage, as database drivers will be loaded.

Maximising Network Performance

When Desktop Surveillance is running in a networked environment, additional aspects need to be considered due to network bandwidth limitations, if surveillance recordings are stored on the network server.

The recording interval on each workstation should be proportional to the number of workstations streaming images to the server over the same network bandwidth. To determine the best setting, use network traffic monitoring tools.

Colour Modes

The lower the colour mode, the less space the recordings will take. The Black&White mode is preferable as it takes up only a fraction of space/memory in comparison with the high colour mode.

Hiding Desktop Surveillance in Windows NT

Hiding the fact that Desktop Surveillance is running from users is not as straight forward in Windows NT as in Windows 95 or 98. Windows NT is created to be a secure operating system and it is not possible to hide running processes from users. If users press Ctrl-Alt-Delete the system will show a Windows NT task screen and running applications will be visible in a task list via the task manager. The solution to this is therefore to remove the possibility for the users to access the task list. This can be done by removing (or renaming) the file

taskmgr.exe

from folder WINNT\system32

User License

A single user license entitles the user to install Desktop Surveillance on one computer only. The option of a multi-user license will let the user install the software on a number of computers in accordance with the license purchased. If the number of computers that have Desktop Surveillance installed exceeds that stated in the registration section, please ensure that the license details are re-entered.

Our pricing policy offers attractive discounts on multi-user licenses. Please see the purchase section on our web site for details: http://www.omniquad.com

The serial number is stored in file ODS.LIC located in the program directory - this file should be always present and the application will revert back to evaluation mode if the license details are not found. The serial number is not stored in the system registry in order to make the software easier to hide from the user.