Omniquad Desktop Surveillance

Step-by-step

DESKTOP SURVEILLANCE: SIMPLE RUN

REAL TIME MONITORING ACROSS THE LOCAL NETWORK OR THE INTERNET.

NETWORK DISTRIBUTION AND NETWORK ADMINISTRATION

DESKTOP SURVEILLANCE: SIMPLE RUN

Follow the instructions below to create and play back sample surveillance records. Please note that the purpose of this section is to show you the basic capabilities of Desktop Surveillance. After you get more familiar with it, you will need to customize it further to suit your own requirements.

1) Create a new folder on your hard disk to store records, for example c:\ records
2) Load Desktop Surveillance user interface from the start menu
3) Select the Options tab and click on the 'RESET INSTALLATION TYPE' button, select option 'LOCAL'
4) Click on the Surveillance Profiles tab. Ensure that only one profile (DEFAULT) is present. Delete any other profiles if present
5) Select the DEFAULT profile and click on the EDIT button – a new dialog will be shown
6) Clear ALL options in ALL sections of the Tabbed properties dialog

Select each tab in turn and set the following settings:

GENERAL
Enable Desktop Surveillance: ON
Allow user to terminate Desktop Surveillance from…: ON

MODES
Settings in this section cannot be customized in the trial version – a warning message will be shown always when Desktop Surveillance is activated

ACTIVITY LOG
Enable Activity Log: ON
Activity Log Folder: C:\RECORDS

TRIGGERS
Record always when this user is logged on: ON

ACCURACY
Set the snap interval to 0 minutes 10 seconds
Color depth: 16 color
Skip Identical Frames: ON

RECODING TO DISK
Save recordings to a disk (or local network): ON
In the text box below, enter C:\RECORDS
Create a new subfolder for each user: ON
Reserve Disk Space (MB): 0

Once you have set all options above, click the OK button and allow the window to close. Click the 'CLOSE' button on the main program window and restart your computer. When Windows loads, there will be a warning message telling you that Desktop Surveillance has been activated (this message cannot be turned off in the trial version).

To double-check that Desktop Surveillance is operating, open folder C:\ RECORDS from windows Explorer. You should see a new folder that is named after the current user. A new sub-folder should be there, and its name would be a combination of date and time when the recording session has started. When you check the contents of this folder, you should see a new file with extension appearing every several seconds. We have now verified that Desktop Surveillance is recording.

For the next several minutes, work with a few different applications, edit some documents, write some mail messages or browse the Internet – just use your computer.

We can now terminate the active Desktop Surveillance agent and playback records. Press CTRL-ALT-DEL once (task list), select task DSA and click on the END TASK button. Please note that in real world situation, you would have the agent active for most of the time, but you would customize situations in which you would want to record users' activities (you would also configure the software not to be displayed in the task at all)

Once you have terminated active Agent, load Desktop Surveillance from the start menu and select the playback tab. Use the navigation controls and browse to folder C:\RECORDS. Now, browse though the middle folder with your user name to folder with name corresponding to the recording date and time (you need to double-click on the folder icons to open them). When you are inside this folder, click on the VIEW button. A 'remote control' playback window will now appear, and you should see a list of items (each one corresponding to a visual record). Click on the > button – you will now see a visual playback of all activities. You can pause the playback and navigate though the recording frames.

Every time any user logs on, Desktop Surveillance would create a new recording folder for them and then create subsequent session folders with their names corresponding the dates when the users have logged on.
In a real word situation, you would change the snap setting interval from 10 seconds to 30,60 or more.

In addition to the visual recording, Desktop Surveillance has also created a text log, outlining all users' activities. In Windows explorer, navigate to folder C:\ RECORDS again – you should see a new file with extension LOG (depending from your system settings, you may not see the extensions at all). Double-click on this file and open it in Notepad – you will see a text summary and times of all activities, including editing document names and browsing the Internet. These records may be optionally stored in a database.

In the full version, Desktop Surveillance also captures all user keystrokes to a file.

REAL TIME MONITORING ACROSS THE LOCAL NETWORK OR THE INTERNET.

Real time network monitoring requires TCP protocol installed (other multi-user features will work with any network protocol). This tutorial assumes that there are 2 workstations:

A – monitored workstation (client)
B – administrator's workstation (master)

The number of monitored workstations is unlimited, and any workstation can be viewed from any network node.

ON WORKSTATION B:

-1 Load Desktop Surveillance user interface from the Start Menu and ensure it is enabled (you can configure the sample settings as explained in section DESKTOP SURVEILLANCE: STEP BY STEP)

Additionally, configure options in the following Tabs:
NETWORK
Enable remote Surveillance: ON
Default port: Leave as 1005

TRIGGERS
Set the 'record always' option off. Although Desktop Surveillance will operate with any combination of preferences, the purpose of this tutorial is to perform network surveillance operations only.

Restart workstation B – when Windows loads, it should display the standard trial-version warning.

ON WORKSTATION A:

-2 First, we need to verify that we really have a network connection to B
-3 Open a DOS window and try to PING workstation B. Depending from your network configuration this can be achieved by using the friendly name or the IP address of B, for example:

PING bcomputername
PING 198.192.0.5
PING bcomputername.ispname.com

A typical naming convention in a local LAN would be ping example 1,2. When operating across the internet, 2,3 naming convention is more likely. Please note that your computer may have more than one set of IP addresses, see the TCP protocol settings in Network Control Panel applet.

You should receive a reply from B as the result of the PING command. If you do not, troubleshoot your network problems and do not proceed further with this Remote Surveillance tutorial, since you do not have a network connection to B.

Once you have verified a valid connection to B, load Desktop Surveillance from the Start Menu on A , select the Network tab from the initial dialog and click on the 'REMOTE SURVEILLANCE' button.

In the top text box, type in the name or IP address of B (use the choice which gave you back results when using the PING command). Now, click on the VIEW button – you will now be presented with the desktop of B and you can periodically refresh the display manually or automatically. Desktop Surveillance interrupts the streams between the workstations, so if you do not refresh display, it will preserve network resources.

Other commands in this dialog will allow you to activate and deactivate local recordings on B.

These are the principles of the basic network surveillance operations. If you need to monitor a large number of users at the same time, enable remote activity log on each client workstation (and enter the computer A name or IP address as the administrator's computer). When you load Activity Monitor from the main Network section, you will be present with a tabular display of all activities on your network.

DESKTOP SURVEILLANCE:
NETWORK DISTRIBUTION AND NETWORK ADMINISTRATION

PART 1: NETWORK DISTRIBUTION

Desktop Surveillance can be rapidly distributed across your network. This manual assumes that there is a sample drive F: , which is mapped on each workstation as a server folder (this can be also a UNC location, such as \\ NTSERVER\LOCAL\C)

1) Unpack the original Desktop Surveillance archive (SPY32.ZIP) into a new folder on the network server drive, for example F:\ODSINST. The folder should be filled in with several compressed files (the last letter of each file extension would be _ (underscore). You should also see file SETUP.EXE
2) On each workstation:

open DOS window and type in the following commands.

F:
CD\ODSINST
setup.exe -s odsinst.log

Desktop Surveillance will be now automatically installed to this workstation. Please note that this is the most basic distribution method.

Alternative 1:
Open NOTEPAD and type in text f:\odsinst\setup.exe -s odsinst.log
Save this document on the F:\ drive as BATCH file – just give it extension BAT instead of TXT, for example ODSINST.BAT
If all your workstations execute the same script on the server upon startup, you can include the batch file in the script itself. You have to remember to reboot any workstation only once if this is the case, so that you will not install the same software several times.

Alternative 2: (preferred)
Use your network distribution system (SMS, LanDesk) to execute f:\odsinst\ setup.exe -s odsinst.log on all workstations simultaneously

PART 2: NETWORK ADMINISTRATION

Once all workstations have Desktop Surveillance installed, you can store all records on the network server, view records from any workstation and change preferences centrally.

In order to achieve this, you need to create a shared network Desktop Surveillance configuration.

1) Create a new folder on drive F:, call it F:\ODS
2) From one of the workstations, copy files

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

   to F:\ODS

   Now we have all the files required for shared network installation – we need to adjust the workstations.
3) On each workstation:

A) modify registry entry:
hkey_local_machine\software\microsoft\windows\currentversion\run\ods25
and change it from the local path to the path of the spn.exe file on the server, adding switch –r, for example entry
hkey_local_machine\software\microsoft\windows\currentversion\run\ods25

You can do this change manually, or execute setstartuppath.exe module (included in admin.zip), with the new path passed as a command line parameter, for example:

setstartuppath.exe F:\ODS\SPN.EXE –R

B) Removing Program Folder

Since Desktop Surveillance will be started from the server, local files are no longer required (since libraries are installed). You can either remove the program folder C:\PROGRAM FILES\ODS manually, or you can execute module removeredundant.exe (included in ADMIN.ZIP)

C) Removing Shortcuts

To remove the program shortcut from the current user's start menu, you can do this manually or execute removeshortcut.exe (included in ADMIN.ZIP)

As with the network deployment, you can combine all 3 commands above into a single batch file. Assuming that you have unpacked ADMIN.ZIP to F:\odsadmin folder, you would create a batch file with the following entries:

F:\ODS\Admin\setstartuppath.exe F:\ODS\SPN.EXE –R
F:\ODS\Admin\removeredundant.exe
F:\ODS\Admin\removeshortcut.exe

As with the network deployment, you can execute this batch file manually or use network distribution tools to execute it on each workstation.

From this point onwards, always load spn.exe from within F:\ODS in order to configure user profiles. The same profile DEFAULT.CFG will be loaded for all users on your network, and you would set the recordings folder as a network path, for example F:\RECORDS. If you want to change settings for just one of the users, create a new profile, named as the corresponding user name.

All users should have rights to create, rename and delete files in the recording folders. In order to ensure that users will never discover surveillance records (accidentally or on purpose), disguise the shared folder among other non-important paths, or preferably, create a hidden network share. A hidden network share is created by adding $ (dollar sign) to the end of the name of any share. A hidden share cannot be seen when network resources are browsed, it can be accessed only directly.