

## Quick Setup Guide

**Before you start:** the `\\server_computer_name\ods$` relates to the network share where Desktop Surveillance is installed. You should always replace it with the real path that reflects the name of computer and share you are using. When installing/configuring on Novell system, replace `\\server_computer_name\ods$` with a mapped volume path, for example `F:\ods`

### Server Installation

Any networked workstation can be used as the server to store data files, but it is highly recommended that you should use the network file server.

- 1) At the file server, start **odse.exe** installation from the product install disk. The product will use a network share, so it is highly recommended that you install it in the root of the server disk volume, for example **C:\ods**
- 2) After the installation is complete, double-click on the 'My Computer' icon and open **C:** drive (or whatever drive you installed the software to). Ensure that the newly created **ods** folder is highlighted and select **sharing** from the **file** menu. In the **sharing** tab, create a new file share named **ods\$** (adding the dollar sign will create an invisible share) and **ensure that all users on the network have full access to it**

To verify that the server files have been installed correctly, go to any network client workstation, select **Run** option in the start menu and type in `\\server_computer_name\ods$readme.txt`. This action should result in the product `readme.txt` being displayed.

Note: `server_computer_name` should be the name of your network file server which will store ODS records. To find out the computer name check the **Identification** tab in the **Control Panel** network section.

### Client Configuration

Note: proceed with the client configuration only after the server installation has been completed. No specific software installation is necessary for the client workstations, each client needs only to start file `odshost.exe` located in the **ods** network share.

Method 1)

Add command `\\server_computer_name\ods$\odshost.exe` to the common network login script

Method 2)

Repeat the following steps on each workstation

Open registry editor **regedit.exe** (select **Run** from the **Start Menu** and type **regedit**). Navigate to section **hkey\_local\_machine\software\microsoft\windows\currentversion\run**, select **New->String Value** from the **file** menu, name it **odsload** and enter same command as listed in method 1 above as the value.

### Test Run

Note: proceed with the test run only after the client configuration has been completed.

Follow the steps below to create and verify a test recording

- 1) Load Profile Editor (**Start Menu->Run**) `\\server_computer_name\ods$\odscfg.exe` from the administrator's workstation
- 2) Select the **DEFAULT** profile and set the following settings:

General:	Enable Desktop Surveillance in this profile: <b>ON</b> Allow remote control and surveillance: <b>ON</b> , enter the administrator's workstation IP address Remove application entry from Windows95/98 task list: <b>OFF</b> Display icon in task tray area: <b>ON</b> Display Message: Enter a test message, such as 'Hello World'
Storage:	Store records on disk: <b>ON</b> Forward records by e-mail: <b>OFF</b> Forward to FTP server: <b>OFF</b>
Logs:	Enable activity logs: <b>ON</b> Activity Log time-out: <b>5</b> Activity Logs path: <code>\\server_computer_name\ods\$</code> Capture Keystrokes: <b>OFF</b>
Virtual Video	Enable Virtual Video: <b>ON</b> Virtual video path: <code>\\server_computer_name\ods\$</code> Record always: <b>ON</b> Skip similar frames: <b>ON</b> Save new frame every...: <b>60</b> (clear any other options on this page)

Clear all options on pages: Executables, Blocking and Lockdown

After selecting all the above options, click on the 'SAVE' button and close the Profile Editor. Next, reboot any workstation that was previously configured for ODS. When the user logs on, message 'Hello World' will be displayed. For next several minutes, use the workstation for the usual tasks.

To assess the records, load (**Start Menu->Run**) `\\server_computer_name\ods$\odisplay.exe` – you should now see a new entry listing user name that was using the test workstation. Double-click on that entry and you should see a new list with at least one item, listing recording session – a combination of computer name and login date. Double click on that entry and the bottom list will display items 0000001, 0000002 – which are the indexed recordings. Click on the play button > to play back the recording.

The second information resource created was the activity log [\\server\\_computer\\_name\ods\\$\odsact.log](#) – this file will store information about activities of all users on the network. This file can be opened in Excel or imported to a database for further analysis.

## Getting Results

### To Record Virtual Video only when users utilise the Internet, IRC (Internet Relay Chat, or access certain applications, documents and web sites.

- 0 Re-enable standard settings (as in the **Test Run** guide section).

In the virtual video section

- 1 Enable option **record only on window or keystroke triggers**.
- 2 Add the names of the applications or documents that you wish to monitor in the **Virtual Video window triggers** list. Each entry should consist of only the text that is always present in the foreground window caption of the application or document you wish to monitor. For example, when users browse the Internet using MS Internet Explorer, the text *'Microsoft Internet Explorer'* will be always present as a part of the application's window title, regardless which web site is opened. The same principle will apply to almost any windows program. Simply load it and see what name is always present as the application's foreground title. To only record when specific documents are opened, enter the document name (not the application name) in the trigger list – most Windows applications display the current document name as part of the application bar caption.

### To Record Virtual Video only when users access illicit/adult content.

- 3 Re-enable standard settings (as in the **Test Run** guide section)

In the virtual video section

- 4 Enable option **record only on window or keystroke triggers**.
- 5 Click on the 'Add Adult' button in the Virtual Video window triggers section. The words related to adult content will be added to the trigger list. If you are concerned about specific topics, you may add the specific words manually. When most adult web sites are accessed, one or more of the trigger words will be displayed in the web browser bar caption.
- 6 You can also trigger Virtual Video when users are typing adult-related phrases on the keyboard (for example during an IRC session or if they search for adult content on the web). Please note: if Virtual Video is triggered on by a keystroke sequence, Desktop Surveillance will keep recording until the user logs off.

### To notify the network manager by e-mail when users access illicit / adult content.

- 7 Re-enable standard settings (as in the **Test Run** guide section).
- 8 Follow the setup instructions **Record Virtual Video only when users access illicit/adult content**.
- 9 In the Storage profile section, enable the option **Forward By E-mail to** and enter the network managers e-mail address. You must also enter the correct SMTP server address (find out in the user's e-mail client settings) as well as the sender's e-mail address.
- 10 When the user accessing the adult content triggers the Virtual Video recording, Desktop Surveillance will automatically forward the recorded e-mail to the relevant address.

### To block access to system settings, applications or documents.

- 11 Re-enable standard settings (as in the **Test Run** guide section).
- 12 In the **Blocking** profile section, enable option 'Block List - Block Match', then add the items that you wish to block to the block list. As with the Virtual Video triggers, the keyword you will need to add is the text that always appears when the relevant application or document is active. For example, to stop the user from being able to change display settings, add keyword **Display Properties**, since this is the text that appears as the window caption on the display settings applet. To stop users from being able to access the Control Panel, add keyword **Control Panel** as the block keyword.