# Omniquad Desktop Surveillance Enterprise User Guide

## Contents

# Introduction

Omniquad Desktop Surveillance offers a unique approach to the implementation of access control, intelligence management, prevention of (and investigation into) the use/misuse of computer equipment and software.

Omniquad Desktop Surveillance addresses not only the issues of web browsing/newsgroups/IRC but also any aspect of local network usage, simultaneously. Various program features recording can be activated as soon as the user visits certain WWW sites or specific IRC channels. Desktop Surveillance can also be remotely controlled, either via a local network or the Internet. In both cases it is possible to remotely observe activity on the local desktop in real time. The program can be applied in a variety of situations - for example to discourage employees from visiting specified WWW sites or performing certain tasks, or to establish organization-wide usage patterns.

# Network Deployment

**Before you start**: the \\server_computer_name\ods$ relates to the network share where ODSE 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

- Designate a system (or network location) to store ODSE records. In most scenarios, the network file server provides a suitable base. On a small network or a peer-to-peer network, this can be practically any workstation.

**Network installation**

At the console of the system designated to store ODSE records, 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**

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 your network have full access rights 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 ODSE 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 only needs 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.

# Step-by-step activity recording and playback

**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
Load Profile Editor (**Start Menu->Run**) \\server_computer_name\ods$\odscfg.exe from the administrator's workstation

Select the **DEFAULT** profile and set the following settings:

General: Enable Desktop Surveillance in this profile: **ON**
Allow remote control and surveillance: **ON** , enter the administrator's workstation IP address
Remove application entry from Windows95/98 task list: **OFF**
Display icon in task tray area: **ON**
Display Message: Enter a test message, such as 'Hello World'
Storage: Store records on disk: **ON**
Forward records by e-mail: **OFF**
Forward to FTP server: **OFF**
Logs: Enable activity logs: **ON**
Activity Log time-out: **5**
Activity Logs path: \\server_computer_name\ods$
Capture Keystrokes: **OFF**
Virtual Video Enable Virtual Video: **ON**
Virtual video path: \\server_computer_name\ods$
Record always: **ON**
Skip similar frames: **ON**
Save new frame every…: **60**
(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 as ODSE client. When the user logs on, message 'Hello World' will be displayed. For next several minutes, use the workstation for the usual tasks.

To assess visual records, load (**Start Menu->Run**) \\server_computer_name\ods$\odsplay.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$\odsact.log – this file will store information about activities of all users on the network. This file can be opened directly from the profile editor (\\server_computer_name\ods$\odscfg.exe) or imported to a database or a spreadsheet application for further analysis.

# User Profiles

When the Omniquad Desktop Surveillance agent loads, it will try to load settings for the currently logged on user. If a profile that corresponds to the current user name cannot be found, the agent will load the DEFAULT user profile (DEFAULT.CFG). Consequently, each user on the network allows can have a unique profile.

Central server installation ensures that a correct profile will be loaded for each user, regardless on which workstation they log on.

## General

**Enable Desktop Surveillance in this profile**
When disabled, Omniquad Desktop Surveillance will automatically unload itself from memory and exit. Use this setting to determine which users are monitored, and which are not.

**Remove application entry from Windows 95/98 task list**
When this setting is enabled, ODSE entry will be removed from the Windows task list. It is highly recommended that this option is always disabled in order to prevent users from being able to terminate ODSE at will.

On Windows NT, the application name will not appear in the task list by default.

**Allow remote control and surveillance**
This setting allows authorized network users to perform the following actions on remote desktops:

-browse file system, upload, download and delete files
-start applications, display web sites and documents
-view local desktops remotely

Before allowing remote control and surveillance, you should consider the associated security risks.

**MultiView host address**
This setting should specify either the friendly name or the IP address of the network administrator's desktop. MultiView allows the authorized user to simultaneously monitor a very large number of users.

On a large network, different user groups can be monitored by different individual users – to achieve this specify different MutliView hosts for various user groups

**Display icon in task tray area**
Displays an 'eye' icon which indicates to the user that the Omniquad Desktop Surveillance agent is active.

**Display message**
Use this option to communicate a start-up message relating to usage policy on your network, for example 'Any activity on this workstation may be monitored' etc.

## Storage

**Store records on disk**
Leaves Virtual Video records to disk. If this setting is disabled, the Virtual Video records will be deleted after they are forwarded away by SMTP or FTP

**Forward by Email to …**
Forwards Virtual Video records to another email recipient. The Omniquad Desktop Surveillance agent will try to send records as soon as connection to the specified SMTP is made. This process takes place in the background.

Virtual Video records are sent as soon as possible. Activity and keystroke logs are sent at 15-minute intervals.

Please see the Maximizing Security section for information about risks associated with Email Forwarding.

**Forward to FTP server**
Forwards Virtual Video records to remote FTP sever. The Omniquad Desktop Surveillance agent will try to send records as soon as connection to the specified SMTP sever is made. This process takes place in the background.

The agent will try to store Virtual Video data in the initial server directory (user ftp root), therefore the FTP account used by the agent should have the necessary permission to create and store files.

Virtual Video records are sent as soon as possible. Activity and keystroke logs are sent at 15-minute intervals.

# Logs

Activity logs store information about dates and times of any applications, files, documents, network resources or web sites accessed by users.  Only the foreground tasks are logged, so a precise record of usage patterns is made.

The records can be easily imported into practically any database system, data-mining program or analyzed directly in a spreadsheet application.

Activity Log data fields:

workstation name
user name
activity start date/time
activity end date/time
activity time span in seconds (time difference between start-end date/time)
activity description (always the same as text taken from the windows task list)

**Enable activity logs**
When enabled, the activity log information is stored in file odsact.log in the specified network paths

**Idle activity time-out**
Assumes that user is away and terminates the log input after a specified number of minutes.

**Capture Keystrokes**
Stores captured keystrokes in file key.log in the specified folder. This function may not work with all applications and may not be compatible with some keystroke monitoring tools.

# Virtual Video

**Enable Virtual Video**
Creates visual records of computer usage. Ensure that the ‘save records to disk’ option is enabled in the **storage** profile section if the records are supposed to be stored permanently.

**Record Always Option**
Ensures that Virtual Video records are always created, regardless of what the user does.

**Record Only on Window or Keystroke triggers**
Please read Window and Keystroke triggers sections for more information on this option.

**Save new frame every …**
Specifies Virtual Video frame interval - the recommended setting is 60 seconds. Intervals below 60 seconds should be applied with caution, so that performance of the clients running ODSE is not affected.

**Enable Secondary Virtual Video timer**
The secondary timer allows you to effectively have 2 recording speeds and should only be enabled with the ‘recording on triggers only’ option on.

The secondary timer can be compared to recording all TV programs, all day, in low-quality ‘Long Play’ mode and recording favorite programs in high-quality ‘Single Play’ mode. For example Virtual Video frames can be taken most of the time every 5 minutes (though the secondary timer), but every 30 seconds when user goes on-line.

**Delete Oldest Virtual Video when disk usage …**
Use this option to maintain a disk space limit for each user profile. Once the limit has been reached, the oldest records will be deleted.

Note: disk space usage is verified on logon only and allows for the limit to be exceeded during the actual login session – in this way, Omniquad Desktop Surveillance can delete the optimum (minimal) number of records. It will have no impact on system or network performance.

**Virtual Video window triggers**
When Virtual Video is in trigger mode, new frames will be taken only when the following criteria are met:

Trigger on list match mode – the caption of the foreground window with the user focus can be matched with the trigger list.

Trigger when no match mode – the caption of the foreground window with the user focus cannot be matched with the trigger list.

Trigger when no match (WWW only) mode – the caption of the foreground window with the user focus cannot be matched with the trigger list, whilst an Internet browser (Internet Explorer or Netscape Navigator) is the foreground application.

If the trigger criteria cannot be satisfied, the Virtual Video will pause and resume once the criteria are.

**Virtual Video keystroke triggers**
Once the user types on the keyboard any of the specified keystroke triggers, the Virtual Video will be turned on permanently until the user logs off.

# Executable window triggers

Starts application/document specified in the **Filename** text box if the caption on the foreground window can be matched with any item in the trigger list.  If the item is a document or a web site, it will be opened with it's default associated application.

Note: the window triggers will be disabled once the first item is triggered.

**Executable keystroke triggers**
Starts the item specified in the **Filename** text box if words typed by the user can be matched with any item in the trigger list.  If the item is a document or a web site, it will be opened with it's default associated application. The keystroke event will be triggered every time the words are matched.

## Blocking

Blocking allows you to deny access to any application, web site or network resource.

**Block List**
When blocking is enabled, the captions of the top level windows are scanned and when the block keyword is matched, the relevant window will be automatically closed.

Example 1)
To stop the user from changing the display properties, add the text DISPLAY PROPERTIES to the block list. When the user logs on next time and tries to open the display properties, that window will be automatically closed (because the text 'Display Properties' appears as a caption in that window)

Almost any activity can be blocked by doing this, since in most cases the caption on the top level window is relevant to that window's content. You may have to display the window first so that you can find out exactly what keywords to add in the blocking list..

**Reverse Block List**
This option can be used instead of the standard block list. Use it only to specify the applications or documents the user is allowed to access – everything else will be automatically closed. The reverse block list can be used to create and enforce very strict policies.

Example 2)
To allow the user access to only excel and no other applications, enable reverse block list and enter word EXCEL into the reverse block list. When the user logs on next time, they will be able to use only Excel - all other activities will be blocked.

**Reverse Block List (WWW only)**
Use to specify a list of internally approved web sites –all other web sites will be blocked. For example, to allow users to browse only the Omniquad web site, enter OMNIQUAD to the reverse block list. Since the text 'Welcome to Omniquad' appears on every page of the Omniquad web site, the users will be allowed to browse freely only within Omniquad web site. If the user tries to load another site, the web browser window will automatically be closed. This list applies to web sites only, so it can be used at the same time as the standard block list.

## Lockdown

**Shut down window triggers**
Shuts the system down if the caption of the foreground window can be matched with any item in the trigger list.

**Shut down keystroke triggers**
Shuts the system down if user types any words that can be matched with items in the trigger list.

# Real-time network monitoring

In order to allow remote operations, each workstation needs to have the ‘Remote Surveillance’ option enabled (and the ODS agent must be active).

Network operations:

**MultiView**
MutliView allows the network administrator to monitor large number of users simultaneously. The IP address of the administrator’s workstation should be specified in the general section of each user profile on the network. When the administrator loads the Remote module, the MutliView list will shortly start displaying log entries for all network users.

Tip: The MultiView feature is especially useful in environments such as educational establishments, where there is a frequent need for the supervisor to efficiently monitor a large number of users at the same time.

**View contents of remote desktops across the network**
In the Remote console, type the friendly name or the IP address of the remote workstation which you wish to connect to. Once the connection is established, click on the View Desktop Button.

**Execute programs**
To execute programs, first connect to remote workstation and then type in the path of the program to execute. Note: the path should be relative, for example if the administrator on computer A enters c:\app.exe to execute on computer B, computer B will try to start the program from it’s own path c:\. Therefore, the path of application to execute should be always be pointing to a network location, for example \\serevername\sharename\appname.exe. By doing this, both computers A and B will start the same application.

**Troubleshooting:**
If the connection to remote workstation cannot be made:
-ensure that the other workstation is on the same TCP/IP network. From DOS window, type PING *workstationname.* If the PING command times out, resolve TCP/IP connection problems before continuing.
-if the connection cannot be made by the remote workstation’s friendly name, try to connect to it by it’s IP address
-ensure that ODS agent is active on the remote workstation and that the remote surveillance option is enabled in the profile of the user currently logged on that workstation

# Large site bandwidth/storage requirements

The exact bandwidth/storage requirements depend on the utilized recording methods and the individual constraints of each network.

In this chapter, the word ‘bandwidth’ relates to the approximate volume of data transferred during a typical 24-hour period on a regular basis and the word ‘storage’ refers to the accumulative volume of data transferred **and stored** since the first recording or the last backup.

## Activity Logs: Very Low Bandwidth

Data stored in an activity log database contains detailed information about all activities that have taken place on each workstation running an ODSE agent.

The Activity Logs consume minimum bandwidth and storage. As each new log entry takes up to 100 bytes, even a large network site would only require a comparatively small amount of network storage.

**Example Activity Log storage usage on a 1,000–workstation site:** Any user can switch between tasks up to 500 times a day (Assuming that each user would intensively use their workstation for 8 hours a day).

(Maximum) Daily volume generated for the example site:
1,000 workstations * 500 log entries from each * 100 bytes each log entry = 50,000,000 bytes
== 47 MB

(Maximum) Annual storage required
260 days * 47 MB = 12 GB

It would not be necessary for an organization to start with the calculated 12GB from day one – space can be added on, as required.

If the log path lies on a compressed NT disk volume, the storage consumption would automatically decrease by a factor of at least 7, since the Activity Log data is stored in a highly-compressive, plain text format. Therefore, it would be feasible to store 1 year’s worth of data for a 1,000-workstation site in about 2 GB.

Activity Log Summary:
The calculations above are provided for exemplary purposes only. The exact volumes are unique to each site and depend on the number of workstations, routing configuration, the bandwidth available on each segment and finally the type of work every computer user does. However, the above example calculation above indicates that even on a heavily utilized network, Activity Log bandwidth and storage consumption are minimal.

## Activity Logs: Off-peak low bandwidth

In situations where adding **any** traffic to an overloaded network is an issue, ODSE profiles should be configured to store the activity logs locally, on each workstation. In this way, activity log records consume no network bandwidth, as they are stored locally on each workstation. During off-peak times (daily, weekly or monthly), data can be copied to the network server. The drawback to this approach, however, is that data stored locally is less secure than the data stored on a network resource.

## Virtual Video: High Bandwidth

Virtual Video records require more storage as they store graphical data. On any workstation with Virtual Video enabled, the bandwidth requirements will vary depending on (in order of importance):

-0 whether the Virtual Video feature is enabled permanently or only in specific situations (for example only when an unauthorized user opens a confidential document or visits a web site with adult content)
-1 the frame interval setting (how often screen the data is saved to disk)

-2 the use of the 'skip similar frames' option which suspends recording if there is no desktop activity
-3 the screen contents (higher bandwidth usage when user is viewing graphics, lower when they work with text or spreadsheets)
-4 the screen resolution

As Virtual Video storage requirements vary in real time, it is not possible to accurately calculate storage requirements. Recording only at certain times (when relevant) can reduce the storage requirements by a factor of up to 100, as compared to recording at all times.

Unlike Activity Logs which achieve high compression rates, there are no real benefits in storing Virtual Video records on a compressed disk volume as Virtual Video data is stored in Portable Network Graphics (PNG) format which is already compressed.

**Virtual Video Scenario 1: continuous Virtual Video recording:**
A 1,000-workstation site, each workstation in continuous use for 8 hours, frame interval setting 1 minute
1,000 workstations * 8 Hours * 60 frames each hour * average 15KB each frame = 7 GB per day (7MB per workstation, per day)

Realistically, it is likely that in this scenario, the site workstations will be used actively for only half of that time (ie. When users are on the phone or screen contents remain the same for 1 minute or longer), therefore the bandwidth and storage requirements would decrease proportionally to 3 - 5GB per day.

This number may appear high initially, however it is offset by possessing a detailed, CCTV-like record of activity of every desktop on a 1,000-node network, which for certain organizations may prove to be a cost-effective security measure.

A realistic low-cost solution to these storage requirements without investing in a large volume of disk drives would be to store data on a backup device every day and then erase the available storage.

If the site, in this scenario, did not have the necessary bandwidth or storage, each profile may be configured to store records locally, then purge oldest data on a regular basis, after a pre-determined storage limit has been exceeded (the same principle can be applied in the network installation).

Tip: By enabling or disabling Virtual Video in different user profiles, the Virtual Video records may then be created only for a small selection of users, resulting in the bandwidth and storage requirements would decreasing proportionally.

**Virtual Video Scenario 2: 'on trigger' recording**

On many networks, it may be not desirable to record Virtual Video for all users at all times. The recording can be limited only to situations that are of particular interest such as:
-5 unauthorized opening of confidential documents
-6 attempts to break into or make an unauthorized copy of an organization's information
-7 accessing illicit content on the Internet
-8 typing certain sensitive keywords on the keyboard
-9 … any additional situation be particularly of interest to an organization

If on a 1,000-workstation site (with recording in example 1) such situations constituted between 1-5% of the total time, the daily bandwidth and storage consumption would range between 70 - 350 MB a day, or 35-150MB with typical computer usage conditions.

**The above calculation assumes that every user on the network would participate in a 'situation of interest' on a daily basis, but in many cases such occurrences will happen randomly, for example some employee gaining unauthorized access to the payroll reports monthly, and another employee accessing illicit content on the Internet 'when nobody is looking'. The storage requirements would therefore decrease accordingly.**

The relatively low storage requirements of 'on trigger' recording combined with the high value of the recorded material make it an attractive monitoring solution.

<u>Virtual Video Summary:</u>
The scenarios above are included for exemplary purposes only and the bandwidth and storage requirements will be almost certainly different for every organization.

# Maximizing security

The nature of Omniquad Desktop Surveillance may demand the application of various security precautions:

-10 Change startup registry entry label from ‘odsload’ to one of your choice.

-11 Rename agent executable from ODSHOST.EXE to one of your choice. This may prove especially helpful on Windows NT in order to make Omniquad Desktop Surveillance less apparent in the process list.

-12 When records need to be forwarded to remote location try using FTP rather than SMTP. Omniquad Desktop Surveillance uses it’s own email engine which bypasses user’s email own email software, but SMTP email can be routed back to the user if there is a network routing failure.

# Case study examples

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

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

In the virtual video section

Enable option **record only on window or keystroke triggers.**
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.

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

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

In the virtual video section

Enable option **record only on window or keystroke triggers.**
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.
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.

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

Re-enable standard settings (as in the **Test Run** guide section).
Follow the setup instructions **Record Virtual Video only when users access illicit/adult content.**
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.
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.

## Block access to system settings, applications or documents.

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