

Illegal View Functionality Listing		Illegal View	
		Professional	Standard
Recording			
Either individual or group setting is selectable		■	■
Monitoring screen recording	Record data on monitoring screen once PC is logged in.	■	■
Multi monitor recording	Record data on multiple monitor screens designated.	■	■
Remote desktop recording	Record monitoring screen of remote desk top (terminal service) session.	■	■
Offline recording	Record data on monitoring screen of corresponding terminals even when the network becomes off.	■	■
Recording interval	Recording interval is adjustable from 1 sec. to 9999 sec.	■	■
Screen color	Selectable from monochrome, 16 colors, 256 colors, high color (16 bits) to true color (24 bits).	■	■
Screen saver	Selectable to record screen saver session or non-record of screen saver session.	■	■
Playback	Selectable from playback, reverse playback, to 6 speed playback and resolution is up to PC.	■	■
Text	Record all text on the monitoring screen.	■	■
Command	Record command prompt execution.	■	■
Key board	Record key stroke on desktop.	■	■
Mouse	Record mouse clicks on desktop.	■	■
Application	Record start and end of applications.	■	■
File access	Record files access by users, applications and OS.	■	■
Status	Record computer status such as log-in, log-out, shut down.	■	■
Resource	Record information of computer hardware, drivers, printers and applications.	■	■
Camera	Record picture images taken by a terminal built in camera or web camera attached to the terminal.	■	■
Real time monitor			
Either individual or user monitoring is selectable		■	-
Real time monitor	Display recorded monitor session in real time (recording interval selectable from 0.5 sec to 5 sec.).	■	-
Remote real time monitor	Display recorded remote desktop monitor session in real time.	■	-
Retrieval			
Either individual or user retrieving is selectable		■	■
Server retrieval	Retrieve history and alert data stored in Illegal View server.	■	■
Alert			
Either individual or user setting is selectable		■	■
System	Detect malfunction of Illegal View server and client if any.	■	■
Application	Detect application start.	■	-
File access	Detect file access.	■	-
Resource	Detect change of computer resource.	■	-
Keyword	Detect registered text in the texts on monitoring screen.	■	-
Removable drive	Detect connection of removable drive.	■	-
Log in	Detect log in terminal and log in user.	■	-
Alert to administrator	Display alert message on management console and e-mail alert information to administrator.	■	■
Logging	Log alert records.	■	■
Operation setting	Set additional recording conditions in addition to standard setting, Lock designated screen, unable to operate.	■	-
Alert to User	Display warning alert message to the monitor screen of corresponding PC.	■	-
Multi-alert	Set up multiple alert conditions and detect corresponding operations.	■	-
Client protection			
Illegal View anti-disable functions		■	■
Stealth	Client program invisible and unstoppable by task manager/windows explore.	■	■
Boot up	Uninstall not allowed when the client program is in operation.	■	■
Observer	Booting up PC not allowed when client program is inoperative.	■	■
Boot up limitation	Booting up PC not allowed when Windows is booted up in safe mode.	■	■
Firewall	When firewall blocks connection with Illegal View server, any use of all digital assets connected to client PC is prohibited.	■	■
Option			
Setting several add-on functions		■	■
Video export	Recorded monitor data are converted into AVI format and export.	■	■
Command Line	Lock terminal screen with command prompt.	■	■
Report	Create original design report format.	■	■
License type			
Encrypt method is now selectable		■	-
Encrypt method	KDTS proprietary encrypted Illegal View and PCI-DSS standard encrypted Illegal View are now available.	■	-

Illegal View <Professional/Standard> Server^(*)2)

OS ^(*)1)	Windows Server 2016, Windows Server 2012R2, Windows Server 2008R2, Windows 8.1 ^(*)3) , Windows 7 ^(*)3)
Recommended ⁽⁺⁾ hardware requirements	CPU : Pentium4 and higher, RAM : 2GByte and more (when recording data with RDP session, requires additionally [2 x virtual client license]MB) HDD : 20 MB for server program, history data volume to be saved ^(*)4) ^(*)5) ^(*)7) ^(*)8) , 500 MB per database file ^(*)9)

^(*)1)Windows 32-bits/64-bits operative, Japanese/English/other local languages Windows OS operative. ^(*)2)Server program requires Microsoft Access 2016 Runtime 32-bit/64-bit. ^(*)3)They are not server OS and so kdts is not responsible for network trouble once Illegal View is deployed operative. ^(*)4)Data transferred from client PC to server PC cannot be recorded if server PC hard disk capacity is full and depleted. ^(*)5)4GByte is maximum recording limit per day per client. And no more recording is allowed if exceeded. ^(*)6)30 MB is the standard recording size per day/ resolution 1,024 x 768 / 8 hours recording/ 16 colors/ every 5 seconds recording. ^(*)7)Up to 5000 users can be registered to one Illegal View server. ^(*)8)Illegal View does not necessarily mean to ensure 100% of operation data recording as it depends upon users' physical and/ or virtual environments and operation environments. ^(*)9)Database file is automatically set up for every 500MByte recording data.

Illegal View <Professional/Standard> Client

OS ^(*)1)	Windows 10, Windows 8.1, Windows 7 ^(*)2) , Windows Vista, Windows XP ^(*)3) , Windows Server 2016, Windows Server 2012R2, Windows Server 2008R2 ^(*)2) , Windows Server 2003R2 ^(*)3)
Recommended ⁽⁺⁾ hardware requirements	CPU : Pentium4 and higher, RAM : 1Gbyte and more (In case of RDP session recording, requires additionally [400 x # of session]KB) HDD : 20 MB for client program use and in case of off line recording, it depends user's requirement ^(*)4) ^(*)5) ^(*)6)

^(*)1)Windows 32-bits/ 64-bits operative, Japanese/English/other local languages Windows OS operative. ^(*)2)Windows security update program (KB3033929) is to be deployed properly for Window 7 and Window server 2008 environment before installing client program. ^(*)3)Some function of illegal view is not operative due to the reason that Windows server 2008 64 bit and Windows Vista are not complied with SHA1. Please consult us in this case. ^(*)4)Client program stops off line recording when Client PC HDD becomes full and no space for further recording. ^(*)5)Illegal View does not necessarily mean to ensure 100% of operation data recording as it depends upon users' physical and/ or virtual environments and operation environments. ^(*)6)Please watch out the HDD open space status all the time as data are recorded to OS system drive.

⁽⁺⁾ Supplementary note:
Hardware requirements Physical and/or virtual environments specifications must meet Illegal View proper operation requirements. Physical and (or) virtual environments ensures proper and rightful operation of Illegal View operative OS mentioned above. Illegal view operative OS is not modified in anyway by physical and/or virtual environments.
Disclaimer / Exemption It is practically impossible to test and ensure the proper illegal view operation for each and all physical and / or virtual environments. Accordingly, we are not responsible for any incidents coming from physical and/or virtual environments. If it should happened to, we do our best to solve the problems but it does not necessarily mean to ensure solving the problems nor revise/modify Illegal View specifications. We make it public such incidents on our home page if we judge that it is appropriate to do so.