2017 - 08

Dell Wyse ThinOS Version 8.4.1 Release Notes

Dell Wyse ThinOS software is designed to run on a broad array of Dell Wyse hardware platforms. New releases are created to support new hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on current, actively shipping hardware platforms, and those hardware platforms that are within their first year after their official End of Life date. Beyond the one year time period, new software releases are no longer certified for use with the older hardware, even though it is possible that they may still work. This allows us to advance our product with features and functions that might not have been supported by the previous hardware, with previous generation CPUs and supporting components.

Current Version: 8.4.1
Release Date: 2014-08
Previous Version: 8.3.2

Contents

Supported platforms

The following table lists the supported hardware platforms:

Platform	Image name
Wyse 3040 thin client with ThinOS	A10Q_wnos
Wyse 3040 thin client with PCoIP	PA10Q_wnos

BIOS information

The following table lists the BIOS information:

Platform	BIOS version
Wyse 3040 thin client	Dell BIOS 1.2.1

New features

This section lists the new features introduced in ThinOS 8.4.1 release:

Package updates

The following package versions are updated along with the new firmware:

- `base.i386.pkg` version number is updated to 4.0.43002.
- `pcoip.i386.pkg` version number is updated to 2.9.43268.

NOTE:

- The last digits in the package version number are for the ThinOS reference and does not match with the application.
- These packages are automatically updated during firmware update. There is no change to package version for the packages that need manual update.

Wireless support

Wireless functionality is supported on Wyse 3040 thin client.

- **Supported Module:** Azurewave AW-CM389MA (Combination of WLAN+Bluetooth)
- **Supported Chipset:** Marvell 8897 chip
- **Supported Standards:** 802.11 a/b/g/n/ac
- **Supported Functions:** Same as other ThinOS products (Roaming and so on)

Bluetooth support

From ThinOS v8.4.1, the Bluetooth feature is supported on Wyse 3040 thin client with ThinOS and Wyse 3040 thin client with PCoIP. Human Interface Devices (HID) and the Headset Bluetooth devices are supported. Also, Bluetooth 4.0 supports Classic and Bluetooth Low Energy (BLE). However, Bluetooth Alternate MAC/PHY (AMP) is not supported.

To know more about the Bluetooth functionality, see *Dell Wyse ThinOS Release 8.4.1 Administrator's Guide*.

For supported peripheral devices, see Peripherals list

Upgrading BIOS on Wyse 3040 thin client

This section describes the procedure to update BIOS on Wyse 3040 thin client with ThinOS, and Wyse 3040 thin client with PCoIP using file server.
The Dell Standard BIOS file is converted to BIN file format for signature and security purposes. The format of the BIN file is, **Wyse_3040_version.bin**.

Updating using file server

To upgrade BIOS using file server, do the following:

1 Download the Dell BIOS file at the Dell support site.
For example, **Wyse_3040_1.2.1.bin**. The BIOS version may be updated in each release.
2 Rename the Dell BIOS file to **A10Q_BIOS.bin**.

3 Upload the renamed BIOS file to folder **WNOS** in the file server—ftp or http(s).
Ensure that the INI parameter **autoload** is enabled for firmware update in **WNOS.INI**.

4 Restart the thin client.
BIOS is updated automatically.

To verify whether the new BIOS is updated correctly, from the desktop menu, click the **System Information** option, or click the **System Information** icon in zero mode. In the **Event Log** tab, the BIOS version log is displayed.
For example, **System Version: 8.4_105 (ROM 1.2.1)**.

This log indicates that the BIOS version is updated to v1.2.1.

BIOS version can be viewed on the BIOS setup screen. To access the BIOS setup, do the following:

1 Restart the thin client, and during system boot, press the `F2` key.
2 Enter the BIOS password, if admin password is set.
3 Click **Settings** > **General** > **System Information**.

The BIOS version is displayed on the screen.

BIOS can be updated by using the Wyse Management Suite console. For more information about Wyse Management Suite, see *Dell Wyse Management Suite Administrator's Guide*.

The following update scenarios are validated for reference:

NOTE:

- Upgrade: Update the firmware to ThinOS 8.4_105 first, and then update the BIOS. This is because BIOS update is only supported from 8.4_105.
- Downgrade: Update the BIOS first, before downgrading ThinOS firmware. This is because BIOS update is only supported from 8.4_105.

Update Firmware and BIOS		Version From	Version To
Upgrade	ThinOS A10Q + BIOS	8.3_210 + 1.0.0	8.4_105 + 1.2.1
Upgrade	ThinOS A10Q + BIOS	8.4_009 + 1.2.0	8.4_105 + 1.2.1
Upgrade	ThinOS PA10Q + BIOS	8.3_210 + 1.0.0	8.4_105 + 1.2.1
Upgrade	ThinOS PA10Q + BIOS	8.4_009 + 1.2.0	8.4_105 + 1.2.1
Downgrade	ThinOS A10Q + BIOS	8.4_105 + 1.2.1	8.3_210 + 1.2.0
Downgrade	ThinOS A10Q + BIOS	8.4_105 + 1.2.1	8.4_009 + 1.2.0
Downgrade	ThinOS PA10Q + BIOS	8.4_105 + 1.2.1	8.3_210 + 1.2.0
Downgrade	ThinOS PA10Q + BIOS	8.4_105 + 1.2.1	8.4_009 + 1.2.0

Configuring BIOS on Wyse 3040 thin client

The following Dell BIOS configurations are supported on Wyse 3040 thin client with ThinOS, and Wyse 3040 thin client with PCoIP using file server (INI parameters):

Table 1. BIOS configuration options

Parameters	Settings
System Configuration	Audio

Security	• Admin Setup Lockout
	• Admin Password
	  • Enable/Disable Admin Password
	  • Update Admin Password

USB Configuration	• Enable Rear-Left Dual USB 2.0 Ports • Enable Front USB Ports

Power Management	• Wake-On-LAN
	  • Disabled
	  • LAN Only
	  • LAN with PXE Boot
	• AC Recovery
	  • Power Off
	  • Power On
	  • Last Power State
	• Auto-On Time
	  • Disabled
	  • Every Day
	  • Weekdays
	  • Select Days

For information about INI parameters and its usage, see INI parameters

For example:

- **Device=DellCmos newpassword=1234567**-Use this INI parameter to create the admin password when password is not set.
- **Device=DellCmos currentpassword=1234567 newpassword=""**-Use this INI parameter to clear the existing password.

INI parameters

The ThinOS v8.4.1 release contains the following newly added INI parameters:

Reference	Description
Service=vncd disable={yes, no} [servers=server_list]	Service=vncd—Configures the service vncd. It is the same as MaxVncd={0, 1} servers option. If you set Service=vncd, it limits the valid vncd client site to the IP addresses in the server_list parameter, which contains IPv4 IP or IP range addresses such as 192.168.1.0/24;192.168.2.48. If you do not set the parameter, all IP addresses are seen as valid.
ResourceURL={yes, no} [Type={Picture}] [URL=_url_path_] [User=_user_name]	The resource files have their specified default path in the file server. For example, the pictures for the **Showing Picture** screen saver are from the folder **/wnos/picture** in the file server. By default, the bitmaps are from **/wnos/bitmap**, and so on. If ResourceURL=yes, the options following it configures one or several resource URLs. The system fetches the resource files from the new URL. If ResourceURL=no, all the options following it is ignored. The option Type specifies the resource type. Currently only the picture which is for the **Showing Picture** screen saver is supported. The option URL specifies a new URL of the resources.

Reference	Description
[Password=_password_] [Encrypt={yes, no}]	The option User and Password specifies the credentials of the new resource URL. The option Encrypt specifies the encryption status of the password. For example, ResourceUrl=yes type=picture url=**ftp://10.151.120.15/pic1** user=pteng password=xxxxxx encrypt=no
Device=DellCmos [CurrentPassword=password] [CurrentPasswordEnc=password encrypted] [NewPassword=password] [NewPasswordEnc=password encrypted] [Audio={yes, no}] [AdminLock={yes, no}] [AutoPower={Disable, Daily, Workday, Days}] [AutoPowerTime=hh:mm] [AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}] [ACRecovery={PowerOff, PowerOn, LastState}] [USBRearPort={yes, no}] [USBFrontPort={yes, no}] [WakeOnLan={Disable, LAN, PXE}]	Device=DellCmos—This option specifies the BIOS settings for the device (Dell Wyse 3040 thin client) using DELL BIOS. CurrentPassword=password—This option provides current BIOS password to change the BIOS settings, if the admin password of the device exists. [CurrentPasswordEnc=password encrypted]—This option is used to encrypt the current password. [NewPassword=password]—This option is used to change the password of the device. (CurrentPassword is not required if admin password of the device does not exist). **NOTE: The encrypted password has higher priority. For example, if both CurrentPassword and CurrentPasswordEnc are configured, CurrentPasswordEnc overwrites the CurrentPassword.** [Audio={yes, no}]—This option controls the activation of the integrated audio controller. BIOS default value is yes. Changing the value becomes effective after you restart the system. [AdminLock={yes, no}]—This option prevents you from entering the setup when an admin password is set. The default value is No. [AutoPower={Disable, Daily, Workday, Days}]— This option sets the time of day when you want the system to turn on automatically. · No/Disable—The system does not automatically power up. · Yes/Daily—The system starts up every day at the time specified in AutoPowerTime. · Workday—The system starts up Monday through Friday at the time specified in AutoPowerTime. · Days—The system starts up on the days specified in AutoPowerDays. [AutoPowerTime=hh:mm]—This option specifies the auto power-on time. Value range of hh is 0–23 while mm is 0–59. [AutoPowerDays—{Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]—This option specifies the days to power up system automatically. For example, Device=DellCmos AutoPower=Days AutoPowerTime=2:30 AutoPowerDays=Sunday; Friday; Saturday [ACRecovery={PowerOff, PowerOn, LastState}]—This option specifies the behavior of the system when the AC power is restored after an AC power loss. · PowerOff—System does not turn on after AC power is restored. · PowerOn—System turns on after AC power is restored. · LastState—System restores the last power state before AC power was removed. [USBRearPort={yes, no}] —If you set USBRearPort to yes, the devices attached to the rear USB port are enabled and available for Operating System (OS). If no is specified, OS cannot see any device attached to rear USB port. [USBFrontPort={yes, no}]—If you set USBFrontPort, the devices attached to the front USB port is enabled and available for OS. If no is specified, OS cannot see any device attached to front USB port.

Reference	Description
	NOTE: **USB keyboard and mouse always work in the BIOS setup irrespective of this setting.** [WakeOnLan={Disable, LAN, PXE}]—The option WakeOnLan allows the computer to turn on from the turn off state when triggered by a special LAN signal. Wakeup from the standby state is unaffected by this setting and must be enabled in the OS. This feature only works when the computer is connected to AC power. • Disable— Do not allow the system to power on by special LAN signals when it receives a wakeup si gnal from the LAN or wireless LAN. • LAN—Allows the system to be turned on by special LAN signals; • PXE— A wakeup packet sent to the system in either the S4 or S5 state causes the system to w akeup and immediately boot to PXE.
ScepAutoEnroll = { yes | no } [Location = location] KeyUsage = key_usage [EnrollPwd = enrollment_password] [EnrollPwdEnc = encrypted_enrollment_password] [ScepAdminUrl = scep_administrator_page_url]	This option is to allow client automatically get certificates and renew certificates using SCEP protocol. ScepAutoEnroll—Set this keyword to yes to enable client's functionality to automatically obtain certificate. RequestURL—This option is to specify the SCEP server's service URL. This field must be set correctly. Do not add any protocol prefix before URL. Currently HTTP is used as the only communication protocol for SCEP requests and security is ensured by SCEP itself. If neither ErollPwd nor ErollPwdEnc is set, client tries to use these set of settings to automatically get an enrollment password and then use that password to request a certificate. If communication security is necessary in your environment during this phase, add “https://” prefix for ScepAdminUrl to use HTTPS instead of the default HTTP protocol.
CCMEnable={yes, no} [CCMServer=server_address[:port]] [GroupPrefix=prefix] [GroupKey=hashkey]	CCMEnable—Yes/no option to enable the Cloud Client Manager Agent. CCMServer—Specifies an IP address or URL address for the CCM server. Default protocol is HTTPS, if "http://" or "https://" is not available. Default port is 443. Once specified, it is saved in the nonvolatile memory. Example: CCMEnable=yes CCMServer=http:// xxx:8080 GroupPrefix and GroupKey—The options GroupPrefix and GroupKey compose the Group Registration Key of the Cloud Client Manager server. Once specified, it is saved in the non-volatile memory. **NOTE: The length of "GroupPrefix" is fixed to 4; the length range of "GroupKey" is 8–31 characters.**

Fixed issues

The following table lists the fixed issues:

CIR number	Description
92308	Citrix application icon refresh reliability changes.
92272	Imprivata fingerprint enrollment changes to support OneSign 5.3.
92220	SR944711153 – Wyse 5010 thin client display port monitors do not wake up after you exit the screen saver.
92173	Connection manager changes to address DNS reliability issues.

CIR number	Description
92100	Wyse 5060 thin client display port improvement to resolve no video issues when reconnecting a monitor after boot.
92078	Central Configuration file server password length increased to 31 characters.
92049	System memory management improvements to avoid out of system heap conditions.
91991	Clients not able to write double-byte characters to USB disk folders or file names.
91945	Clients not able to write double-byte characters to USB disk folders or file names.
91926	RDP h.264 can result in grey display blocks after a period of use.
91923	UNI II extended wireless channels for the Sparklan wireless module is supported.
91919	Window management is enhanced to improve reliability.
91909	Copy and paste button is supported for Contour Roller Mouse Pro 2.
91883	DNS values defined in the user interface were being replaced instead of added to DHCP DNS values.
91865	Wireless management improvements to avoid out of system heap conditions.
91849	RDP h.264 can result in grey display blocks after a period of us.e
91816	Addressed issues preventing the disable mouse parameter from functioning properly.
91815	Wyse 5010 thin client unable to re-sync with a display port monitor powered on after client boot.
91782	SR944202561 – 5060 AutoSignoff=Yes Reboot=Yes would shutdown instead of reboot.
91766	Imprivata changes to address tapover and suspend action (SignOn/Lock) issues.
91764	VNC accept improvements to ensure the timer would only be called once per VNC session.
91762	When Sysmode=VDI and the username field is disabled, Admin Mode username could not be entered.
91692	Added a new command to hide the VmWare View server URL on the logon screen.
91619	Added a new command for Citrix to control the color of the "Enter Credentials to Logon" message.
91574	Resolved an issue that would result in a Citrix Self-Service Password reset challenge question delay.
91562	Citrix storefront/session connections using smartcards could result in invalid pin or certificate not found.
91555	Wyse 5010 thin client default USB com port assignments were not associated to the correct USB port.
91465	SR942627825 – RTAV libraries update to improve session reliability.
91463	Wyse 3020 thin client OS improvements to improve client reliability.
91436	Improved monitor handling to avoid reboot prompts when exiting screensaver.
91423	Wyse 3010 thin client Citrix RAVE improvements.

CIR number	Description
91405	Added support to control the CCM check-in interval after a check-in failure.
91403	Added FIPS level 2/3 support to resolve an issue where newer Gemalto smartcards were not recognized.
91379	Improved Imprivata support to avoid client lockups when performing a tapover from a locked client.
91378	RDP h.264 can result in grey display blocks after a period of use.
91309	Enhanced the client to allow for the support of Defaultini settings when using SelectGroup.
91306	Cherry keyboard smartcard reader name format change to be consistent with Windows based clients.
91286	Moved desktop images out of system memory to allow for support of large uncompressed bitmaps.
91264	Addressed an issue where VNC should show two monitors when only one monitor was attached.
91222	Added support to allow smartcard removal behavior to function with shutdown counters.
91149	RDP h.264 can result in grey display blocks after a period of use.
91090	Resolved issue that prevented SelectserverList=PNA use with CCM.
91051	Fixed an issue preventing the recognition of magnetic card reader.
90863	Improved Citrix Windows Media Redirection experience by changing the video processing order.
90810	Changed OHCI audio handling to avoid issues encountered when a transfer was aborted.
90715	Improved client reliability when using RTME to make calls between two client devices.
90691	Improved client reliability when using a Citrix with a Bloomberg keyboard in a Windows 10 virtual machine.
90501	Fixed a large RDP UDP PDU header problem that prevented PPT slideshows execution in a session.
90498	Resolved network issue pertaining to IPv6 initialization when IPv6 was not enabled .
90474	RDP h.264 can result in grey display blocks after a period of use.
90396	Added code to improve RDP session sharing when using vWorkspace.
90381	Added VPN connection support to prompt for password when a password is not defined.
90307	RDP h.264 can result in grey display blocks after a period of use.
90301	RDP h.264 can result in grey display blocks after a period of use.
90253	SR2895764 – Added support for the Oberthur ID-ONE PIV smartcard with OmniKey 3021 readers.
90153	RDP h.264 can result in grey display blocks after a period of use.
90103	RDP h.264 can result in grey display blocks after a period of use.
90002	Improved wireless reliability to avoid PCoIP “network congested” messages.

CIR number	Description
89726	RDP h.264 can result in grey display blocks after a period of use.
89587	Resolved Horizon disconnect issue after 20 hours by adding “Forcibly disconnect users set to Never”.
89281	Added “RequireSmartCard=optional” to allow for optional smartcard authentication at SignOn.
88616	RDP h.264 can result in grey display blocks after a period of use.
88244	RDP h.264 can result in grey display blocks after a period of use.
87162	RDP h.264 can result in grey display blocks after a period of use.
80884	Added VerifySignature support to allow for firmware integrity checking on Wyse 3010 thin clients.

Known issue

None

Testing environment

The following tables display the testing environment for the respective attributes:

CCM	3.0
WMS	1.0
WDM	5.7.2
Imprivata	5.2.0.15
Caradigm	6.3.1.17
NetScaler	9.3/10.0/10.1/10.5/11.0/11.1
NetScaler Insight Center	11.1
Store Front	2.6/3.6/3.8/3.9
Web Interface	5.4
SecureMatrix	4.1.0

	Win 7	Win 8.1	Win 10	Linux	W2K8R2	W2K12R2	W2K16	APPs
VMware Horizon 7.0/7.1	√	√	√	√	√	√	√	√
XenDesktop 5.6	√							
XenApp 6.5					√			√
XenDesktop/XenApp 7.6	√	√		RedHat 6.6	√	√		√

	Win 7	Win 8.1	Win 10	Linux	W2K8R2	W2K12R2	W2K16	APPs
XenDesktop/XenApp 7.13	√	√	√		√	√	√	√
RDS 2012 R2	√	√	√			√	√	√
RDS 2016							√	√
Teradici PCM 1.03 for AWS	√							

NOTE: AWS Workspace VM OS Windows 7 style is based on 2008 R2 RDSH.

XenDesktop/ XenApp	Operating System	RTME	Lync client	Lync server	Skype for Business (SFB) server
7.13	Windows 7	2.2	SFB 2015		SFB 2015
	Windows 8.1	2.2	SFB 2015		SFB 2015
	Windows 10	2.2	SFB 2015		SFB 2015

Peripherals list

This section lists the supported peripheral devices and peripheral eco system.

Table 2. Peripheral devices

Keyboard/ Mouse
Dell KM636 Wireless Keyboard and Mouse
DELL Wireless Keyboard/ Mouse KM632
DELL Wireless Keyboard/ Mouse KM714
Dell Keyboard KB216p / Mouse MS-116p
Dell Mouse MS111-P
Dell Keyboard KB113p
Dell Keyboard KB212-B
Thinkpad Compact Bluetooth Keyboard
Rapoo E6100, Bluetooth
Dell Wireless Mouse – WM324
Dell Optical Wireless Mouse – WM123
Dell WM713 Bluetooth
Logitech Ultrathin Touch Mouse T630, Bluetooth

Logitech K380 Keyboard, Bluetooth
Microsoft ARC touch mouse 1592, Bluetooth
SpaceNavigator 3D Space Mouse
Logitech M310 Wireless mouse
Dell keyboard KB216P
Logitech K480 Keyboard, Bluetooth
Microsoft Arc Touch Mouse 1428
Microsoft Designer Bluetooth Keyboard/Mouse
Logitech M557 mouse, Bluetooth
USB Webcam
Logitech C920 HD Pro Webcam
Logitech C930e HD Webcam
Logitech C270 HD Webcam
Logitech C525 HD Webcam
Logitech USB Webcam 9000
Microsoft LifeCam 3.0 Cinema
Microsoft LifeCam HD-3000
Microsoft LifeCam Studio
Printer
Dell B2375dnf Mono Laser Multifunction Printer
HP LaserJet P2035
EPSON PLQ-20K
HP Color LaserJet CM1312MFP
Mobile device
iPhone 6
HTC one-XL
Samsung Galaxy S7
USB Disk

SanDisk Extreme USB 3.0 16G
SanDisk Cruzer 8 GB
SanDisk USB 3.0 16 GB
Kingston DataTraveler 100 G3
Kingston DataTraveler G3 16GB
Kingston DataTraveler G3 8GB
Kingston DataTraveler Elite 3.0 16G
Kingston DTM30 32GB
Kingston Mini Fun 8GB
ADATA S107/16GB
ADATA UV150 USB 3.0 16GB
PNY USB3.0 16GB
USB Headset
Jabra PRO 9450
Jabra Speak 510 MS, Bluetooth
Jabra SUPREME UC MS /LINK 360, Bluetooth
Jabra PRO 9470, Bluetooth
Jabra UC Voice 550 MS Duo
Jabra BIZ 2300 Duo, USB, MS
Jabra UC Voice 750MS Duo Drk
Plantronics BLACKWIRE C435-M
Plantronics BLACKWIRE C520
Plantronics BLACKWIRE C710, BlueTooth
Plantronics Voyager Legend UC B235 NA, Bluetooth
Plantronics DA45
Plantronics SupraPlus HW251N
Plantronics DA60
Plantronics P420

Plantronics W440,SAVI,CONVERTIBLE,DECT 6.0(D100)
Plantronics Calisto P240 D1K3 USB handset
Plantronics Calisto 620-M, bluetooth
Plantronics USB DSP DA40(B)
Plantronics 655 DSP
Plantronics List Savi 400 series
SENNHEISER SP 20 ML Speakerphone for Lync and mobile devices
SENNHEISER SC 660 Binaural CC&O HS, ED
SENNHEISER SC 260 USB MS II
SENNHEISER SP 10 ML Speakerphone for Lync
SENNHEISER D 10 USB ML-US Wireless DECT Headset
SENNHEISER SC 260 USB MS II
SENNHEISER SC 75 USB MS
POLYCOM Deskphone CX300
Logitech h150
EDIFIER
Monitor
Dell E1715s—1280 x 1024
Dell E2416Hb—1920 x 1080
Dell ST24—1920 x 1080
Dell UZ2315H—1920 x 1080
Dell D2215Hc—1920 x 1080
Dell U2414HB—1920 x 1080
Dell S2415H—1920 x 1080
Dell U2415—1920 x 1200
Dell U2412M—1920 x 1200
Dell U2913 WM—2560 x 1080
Dell U2713Hb—2560 x 1440

Dell U2713HM—2560 x 1440
Dell U2713HMt—2560 x 1440
Dell ST2420L—1920 x 1080
Dell 3008WFP—2560 x 1600
Dell U3014t —2560 x 1600
Dell P2715Q—3840 x 2160
DVD ROM
BENQ DVD Drive
Samsung Portable DVD Writer SE-208
Dell DW316
Samsung Portable DVD Writer SE-208
Smart card Reader
Dell Keyboard SK-3205—Smart card reader
Dell Keyboard M/N KB813—Smart card reader
HID OMNIKEY 3021
OMNIKEY OK CardMan3121
HID OMNIKEY 3021
Cherry keyboard RS 6600 with smart card
Cherry keyboard RS 6700 with smart card
Smart card
ActivIdentity V1
ActivIdentity V1 (Gemalto IDClassic 230)
ActivIdentity V2
Gemalto/IDPrime.NET (Gemalto .net 510)
Gemalto ID Prime MD v 4.0.2 (840)
Gemalto ID Prime MD v 4.1.0 (3810)
Gemalto ID Prime MD v 4.1.1 (830)
Gemalto ID Prime MD v 4.3.5 (830)

Etoken CardOS
Etoken CardOS (white USB key)
Etoken Java(aladdin) (blue USB key, eToken PRO Java 72K OS755)
Etoken Java(aladdin) (black USB key, SafeNet eToken 510x)
Etoken Java(aladdin) (black USB key, SafeNet eToken 5110)
A.E.T. Europe B.V. (SafeSign)
PIV (Yubico) (black USB key)
cv cryptovision gmbh (c) v1.0ns
Others
Elo Touch Screen Serial
Prolific USB-to-Serial converter U232-P9V2
Dell S2240T(Touch)
USB-to-Serial converter
Dell DP-VGA convertor
Dell DP-DVI KKMYD convertor