

Dell Wyse ThinOS Lite 2.5_009

Release Notes

Current Version: 2.5_009

Release Date: 2018-02

Previous Version: 2.4_112

Copyright © 2018 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.



Contents

Importance.....	3
Current Version	3
Previous version	3
Platform and BIOS information	3
New features	3
Platform matrix	3
Package update	4
BIOS update details	4
GUI# 1 First Boot Wizard.....	5
GUI #2 System information.....	11
GUI #3 Trap picture export	11
Citrix #1 Multiple audio device support	12
Citrix #2 NetScaler + SMS PASSCODE authentication (CensorNet MFA).....	14
Citrix #3 RTME/RTOP 2.3.....	16
Network settings change without reboot	16
Wyse Device Manager/Wyse Management Suite changes.....	17
Troubleshooting.....	20
INI parameters.....	21
Fixed issues.....	23
Test environment.....	23
Tested peripherals.....	24

Importance

RECOMMENDED: Dell recommends applying this update during your next scheduled release cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers and software).

Dell Wyse ThinOS Lite 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

ThinOS Lite 2.5_009

Previous version

ThinOS Lite 2.4_112

Platform and BIOS information

The following table lists the supported hardware platforms:

Table 1. Supported platforms

Platform name	Firmware (ThinOS lite/zero for Citrix)	BIOS version
Wyse 5010 zero client with Citrix	ZD00_xen	3.0 U
Wyse 3020 zero client with Citrix	T00D_xen	w-loader 7.0_216
Wyse 3010 zero client with Citrix	T00_xen.bin	EC 3.02

New features

The following are the new features in this release:

Platform matrix

The following table lists the new features for the thin clients:

Table 2. New feature platform matrix

New Feature Platform Matrix	Wyse 5010 zero client	Wyse 3020 zero client	Wyse 3010 zero client
Package update	Yes	Base package only	Base package only
BIOS update	3.0U	No update	No update
GUI#1 First Boot Wizard	Yes	Yes	Yes
GUI#2 System Information	Yes	Yes	Yes
GUI#3 Trouble Shooting	Yes	Yes	Yes
Citrix Multiple Audio	Yes	NA	NA
Citrix NetScaler + SMS PASSCODE	Yes	YES	Yes
Network Setting without reboot	Yes	Yes	Yes
WDM/WMS	Yes	Yes	Yes

Package update

- Auto update following firmware update
 - Base.i386.pkg: updated to 5.0.46515 for new firmware version
- Self-install or update without the INI
 - RTME.i386.pkg: updated to 2.3.44433 following RTOP 2.3 from 8.4_110
- Require INI to install or update (see Admin Guide)
 - FR.i386.pkg: updated to 1.20.46089

NOTE: The suffix (xxxx) in the package file names version number is for ThinOS Lite and does not refer the application version.

BIOS update details

- New BIOS fixed issues
 - Beep issue
 - Password token support
 - Unexpected boot issue (for Wyse BIOS)
- To make BIOS management consistent between Wyse and Dell BIOS, new INI parameters are added in Device=Cmos for Wyse BIOS
 - [AutoPowerDate={yes, no}]
[AutoPowerTime=hh:mm:ss]
[AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]
 - [CurrentPassword=password]
[CurrentPasswordEnc=password encrypted]
[NewPassword=password] [NewPasswordEnc=password encrypted]

NOTE: Refer to INI parameters section and INI guide for complete details.

- For BIOS configuration, if a password is configured, the password is required to update any settings. For example, the INI parameter to update settings must be same as CurrentPassword={}. This is mandatory for Dell BIOS, and will be implemented as mandatory for Wyse BIOS post this release.
- After a File Server BIOS update to a Wyse 5010 thin client device, due to a CMOS mismatch, BIOS management may not be possible till the user manually enters and exits the BIOS configuration menu. This can be accomplished as follows:
 - Boot unit and press **Delete** during boot to enter BIOS menu.
 - Enter the BIOS password.
 - Press **F10** to save BIOS configurations and resolve the CMOS mismatch.

The following table contains details on the main BIOS function and support matrix:

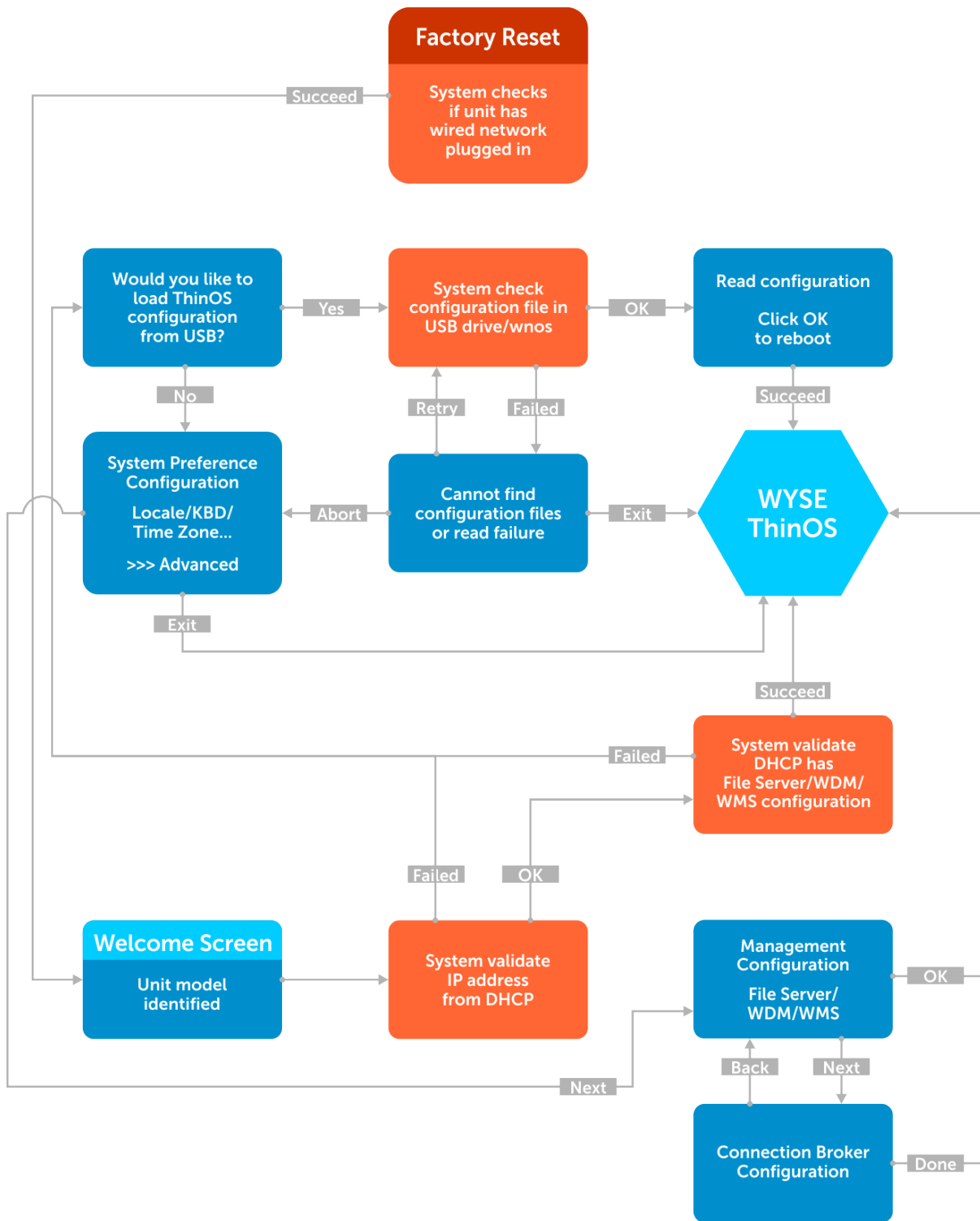
Table 3. BIOS function matrix

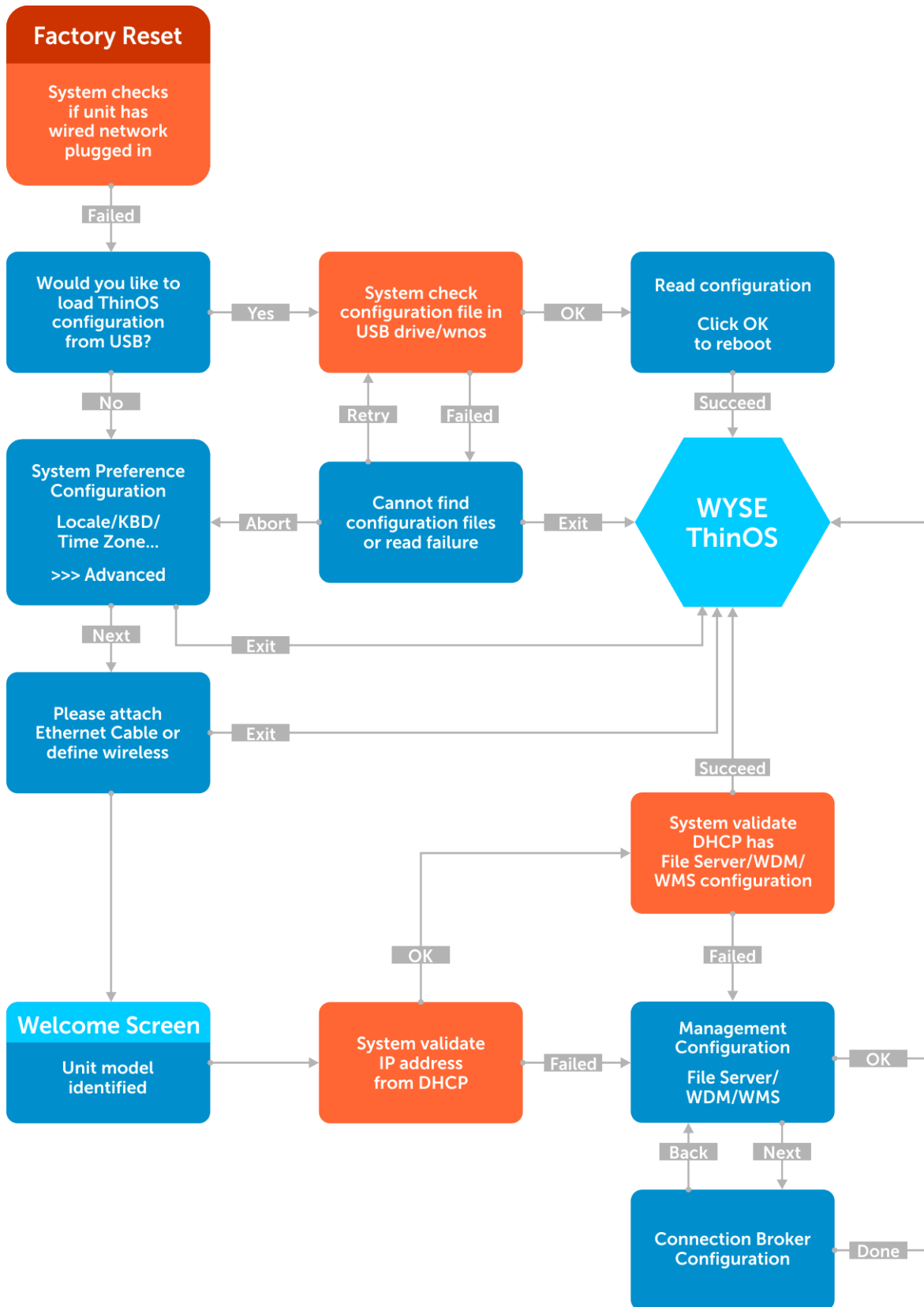
Major Requirement	INI example for BIOS management	Wyse 5010 zero client 3.0 U
Power on without beeps	NA	Yes
Update BIOS from file server	NA	Yes
Change BIOS password with INI	Device=Cmos CurrentPassword={} NewPassword={}	Yes
Change boot order with INI	Device=cmos BootOrder={PXE, HardDisk, USB}	Yes

Enable/Disable USB imaging with INI	Device=cmos BootFromUSB={yes, no}	Yes
Manage AC recovery with INI	Device=cmos AutoPower={yes, no}	Yes
Manage auto on time with INI	Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday	Yes
CMOS Extract and Restore	Device=cmos Action={extract, restore}	Yes
Audio management with INI	Device=cmos OnboardAudio={yes, no}	Yes
USB Port management with INI	Device=cmos USBController={yes, no}	Yes
Wake On LAN	Device=cmos WakeOnLan= {yes, no}	Yes

GUI# 1 First Boot Wizard

The following flowcharts depict the workflow of the First Boot Wizard:





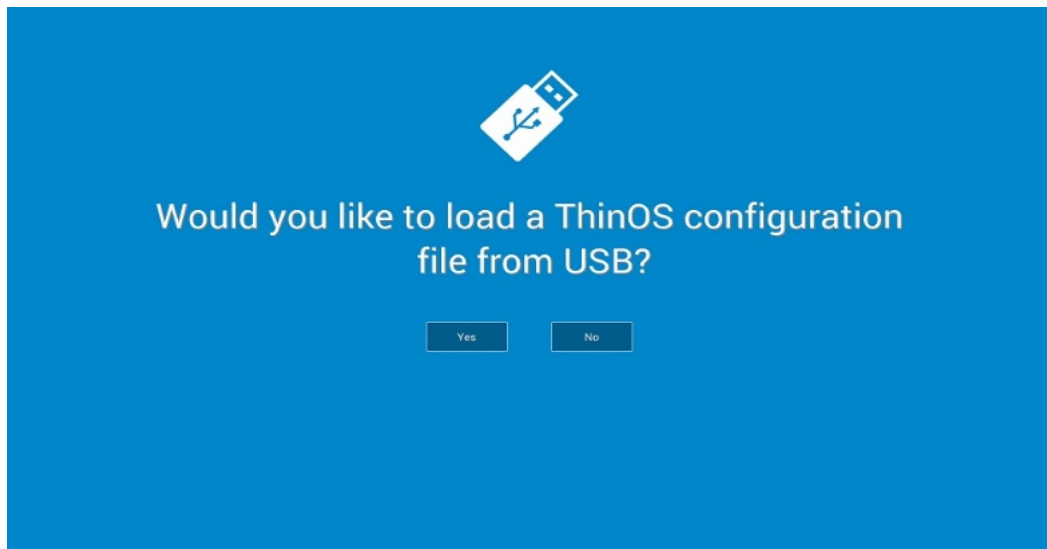
To exit First Boot Wizard

To exit First Boot Wizard, follow these steps:

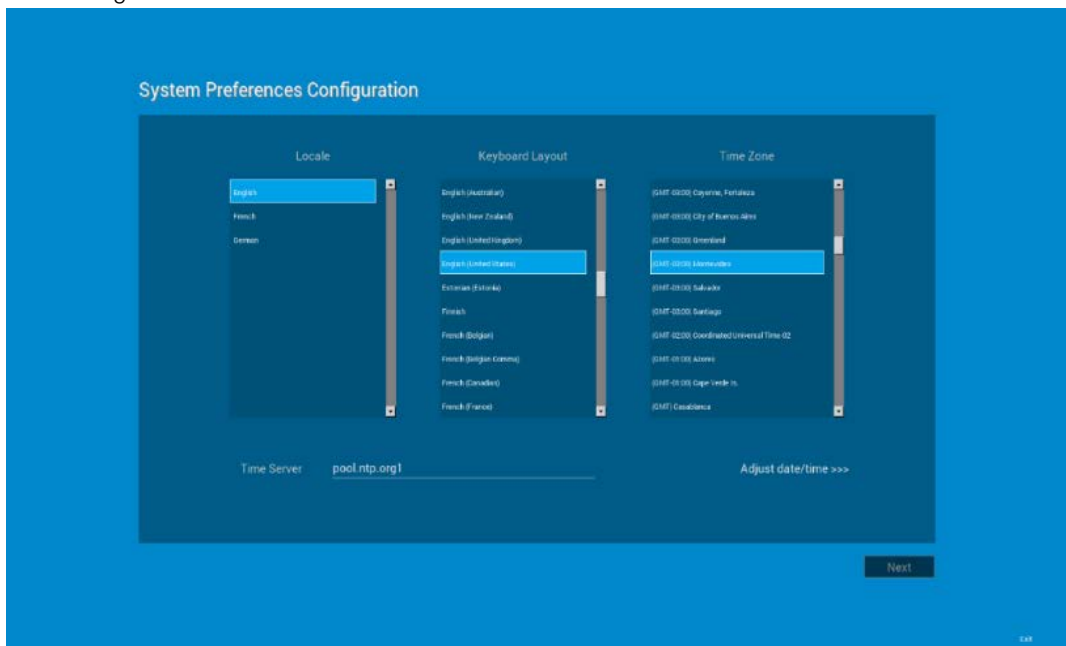
- Select **Exit** at right bottom corner of the following screens:
 - USB config load failure
 - System Preference
 - Ethernet
- Select **OK** or **Done** in the following screens:
 - Read USB configuration success
 - Management Configuration
 - Connection Broker
- Press **Ctrl+Esc** during network connection. You also press **Ctrl+Esc** in the **Welcome** screen to exit First Boot Wizard.

Screen usage and tips

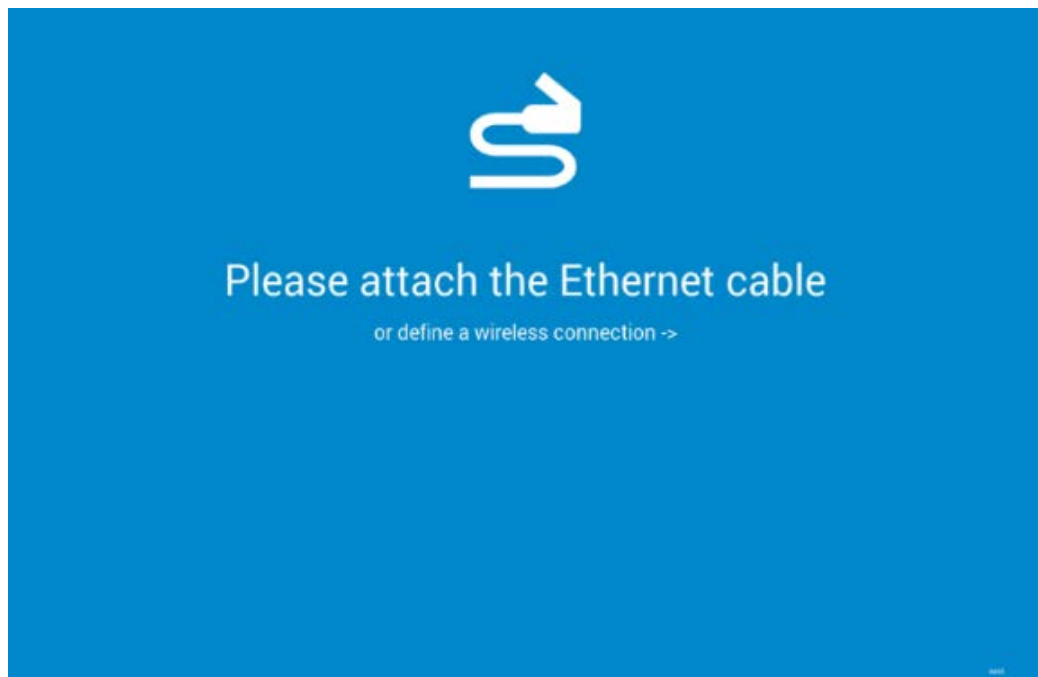
- This wizard is initiated for new units from factory or after factory default reset
- German localization is included in the standard image. The Japanese translation is included in the Japanese image. For including other languages work with MSG file and INI.
- The **Welcome** screen displays the thin client unit model.
- Load USB configuration searches for configuration files such as xen.ini and so on in USB /xen
 - All configuration files can be loaded except for the firmware and package update files.

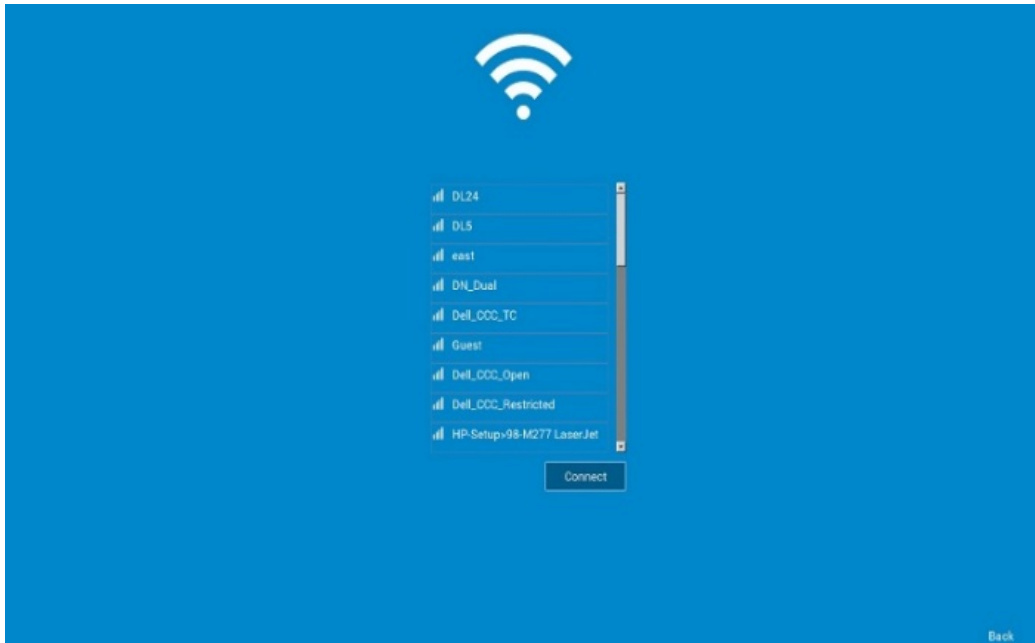


- o On the System Preference Configuration screen select **advanced>>>** to enable daylight saving and so on.

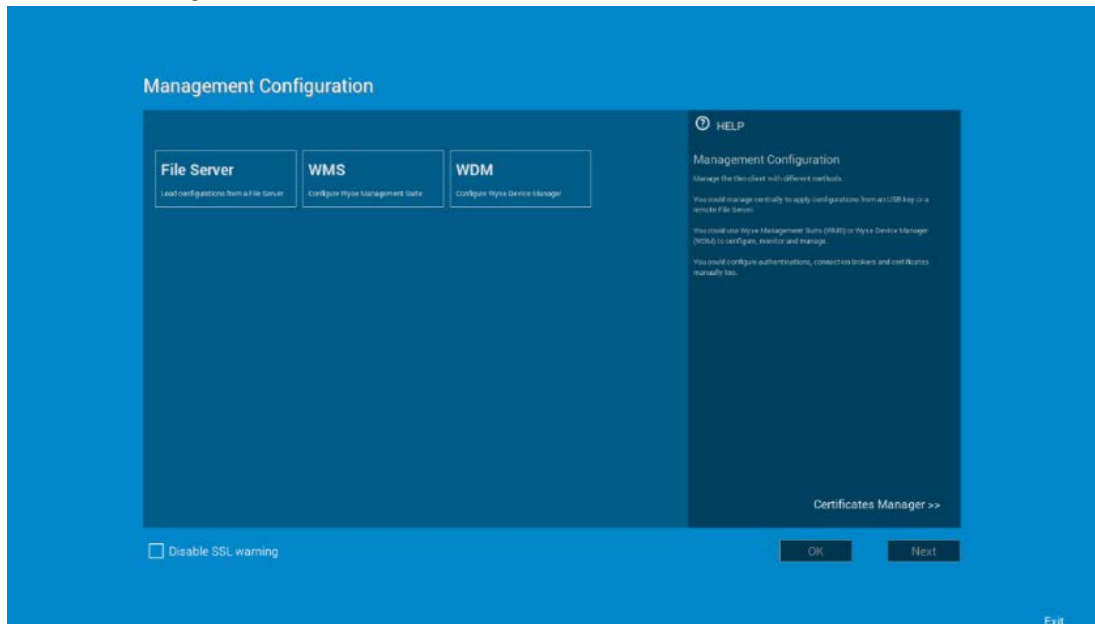


- o On the Attach Ethernet screen, if there is no Ethernet, select **Define a wireless connection** to setup wireless connection. **Define a wireless connection** option is disabled if the thin client does not have a wireless module.





- Management Configuration—File Server, WDM, WMS
 - Additional options such as **Certificate Manager** and **Disable SSL warning** are available.
 - Finish configuration using one of the following options:
 - File Server
 - WDM
 - WMS
 - The system displays the **Done** and **Next** options.
 - Select **Next** to navigate to the next screen where all the manually entered configurations are cleared.



Connection Broker Configuration

- Additional options such as **Certificate Manager** and **Disable SSL warning** are available.

- ThinOS Lite—Citrix

GUI #2 System information

About tab is added in the System Information screen with the following details:

- ThinOS Lite and BIOS image names are added.
- Citrix Broker/Receiver client version is displayed. This represents the ICA revisions between the two ThinOS Lite versions.
- Authentication versions (Imprivata, Secure Matrix, Caradigm, HealthCast)

Firmware reference details

Platform	Firmware
Wyse 3010 zero client	T00_xen.bin
Wyse 3020 zero client	T00D_xen.bin
Wyse 5010 zero client	ZD00_xen

Version conversion information

- Kernel mode –components are implemented in the kernel according to the required specification. The version is displayed as **[max].[min]** which is the base version of protocol or server or client of the component. For example, Imprivata version is 5.2.
- User mode –components are from the source or binary from third party and compiled or integrated into ThinOS Lite. The version is displayed as **[max].[min].[svn_revision]**. The **[max]** and **[min]** is the base version of the third party component, and the **[svn_revision]** is the source control revision of ThinOS Lite. Using this version, you can identify different revisions. For example, Citrix Receiver version is 14.0.44705. The components are actually matched to the installed packages. If the packages are removed, the field will be empty in the **About** tab.

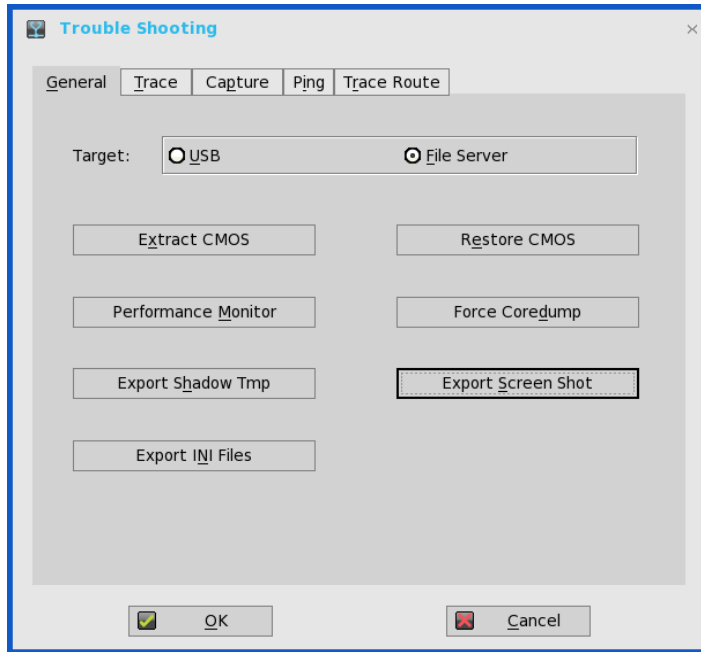
GUI #3 Trap picture export

Provides ability to save trap screenshots to USB/File server and export **xen.ini/ccm.ini** to the USB/File server.

- When a trap occurs, it is no longer necessary to take screen capture.
- Exported file name is added with the build information which is used in troubleshooting.
- Files are uploaded to a file server or USB key in the directory **/xen/troubleshoot/**

Working scenario

- Go to **Trouble Shooting > Export Screen Shot**, the screen shots are exported to file server or USB key.
 - If there is screen shot is copied to clipboard, the screen shot will be exported.
 - If no screen shot is copied to clipboard, it automatically copies full screen and export.
- Go to **Trouble Shooting > Export INI Files**, the global INI file (**xen.ini** or **xen.ini**), **wdm.ini** or **ccm.ini** are exported to a file server or USB key (all INI parameters in the **ccm.ini/wdm.ini/xen.ini** tab are exported).
- Go to **Trouble Shooting > click Force Coredump**, the coredump file and the trap information picture are saved to a local disk. Reboot unit, coredump file and picture file will be uploaded to a file server or USB key.



Citrix #1 Multiple audio device support

- Citrix revision in ThinOS Lite is updated to support the following Citrix new features/changes. See, Citrix version in the **System Information > About** tab for the revision changes.
- Supporting multiple audio device utilization in XD/XA 7.6 and later.

Pre-condition

- Citrix VDI desktops—configuration is not required
- Citrix RDS desktops—policy **Audio Plug N Play = allowed**. By default it is allowed.

Support Devices

- USB headset, webcam (without USB redirection)
- Analog headset

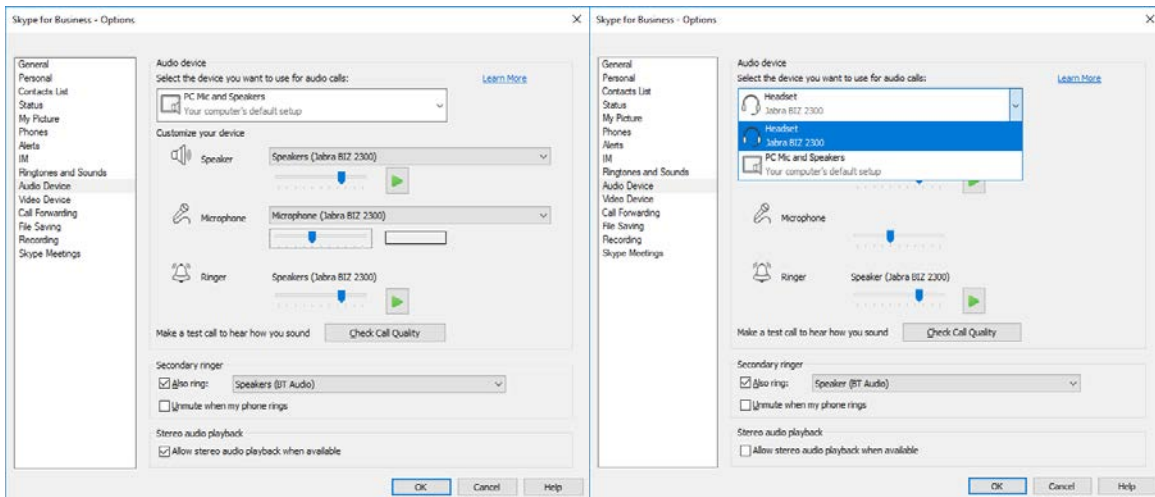
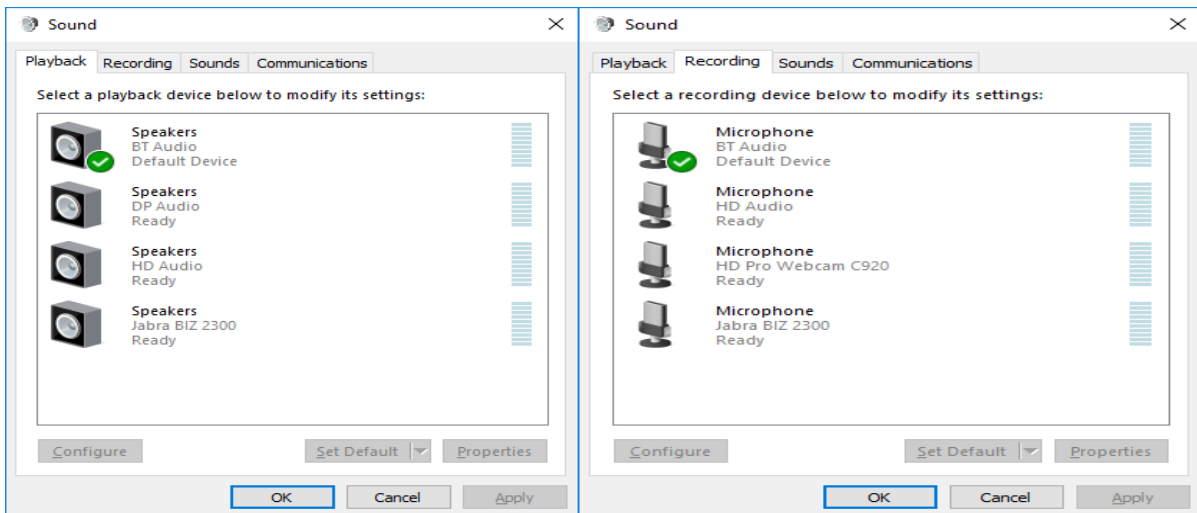
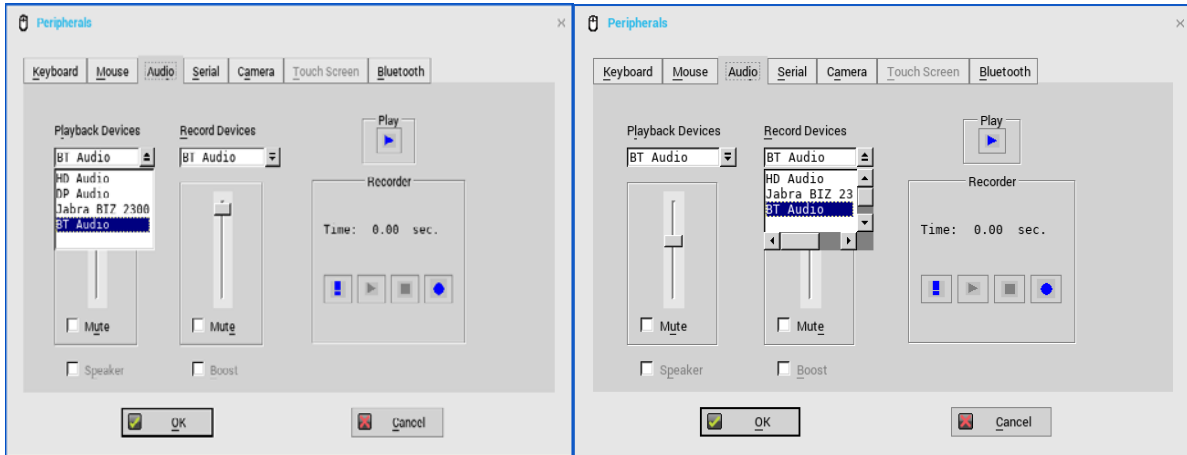
Limitation

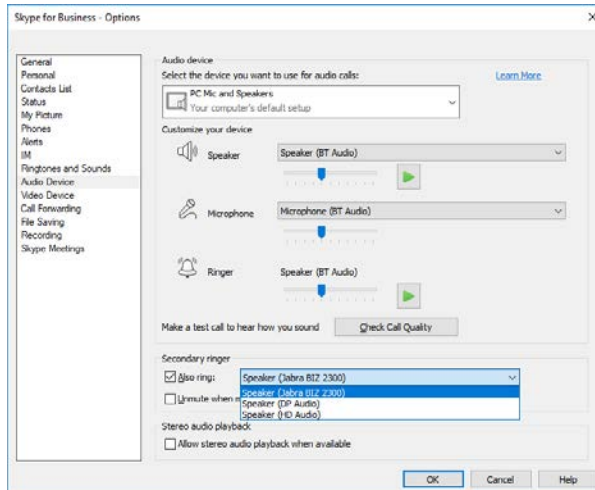
- ThinOS Lite 3010 and 3020 are not supported.
- Citrix multiple audio feature does not work with HDX generic audio. The resolution for the issue will be delivered in the next ThinOS Lite release.

For Citrix multiple audio, you must consider the following points:

- With HDX Generic Audio
 - Audio device—**PC Mic and Speaker**
 - Configure Speaker/Microphone respectively
 - Secondary ringer—audio devices excluding above selected ones
- With RTME
 - Audio device—HID headset + PC Mic and Speaker
 - Set **PC Mic and Speaker** to configure Speaker/Microphone respectively
 - Secondary ringer—audio devices excluding above selected ones
- Tips to work effectively

- o ThinOS Lite default audio = latest plug-in audio device.
- o Session default audio = ThinOS Lite default audio; can be changed.
- o Upon hot plug-in/out device, advise to restart SFB/Lync client.
- o UDP Audio is supported with multiple audio.
- o You can switch audio device setting without hot plug-in/out during a call
- o The multiple audio option can be shared across multiple sessions






Citrix #2 NetScaler + SMS PASSCODE authentication (CensorNet MFA)

- NetScaler 12.0 and later—SMS PASSCODE 9.0 SP1 + RADIUS. To download SMS PASSCODE 9.0 SP1, see <https://download.smspsscode.com/public/6260/SmsPasscode-900sp1.zip>
- Test message works with CensorNet App on mobile
- NetScaler RADIUS authentication policy bind with gateway server.

Do the following for SMS PASSCODE authentication:

1. From ThinOS Lite, connect to NetScaler Gateway URL
2. Enter valid user ID and password.
3. Continue with the Passcode prompt.
4. Get the passcode from CensorNet App on mobile.
5. Enter the Passcode to complete the authentication.



User name:

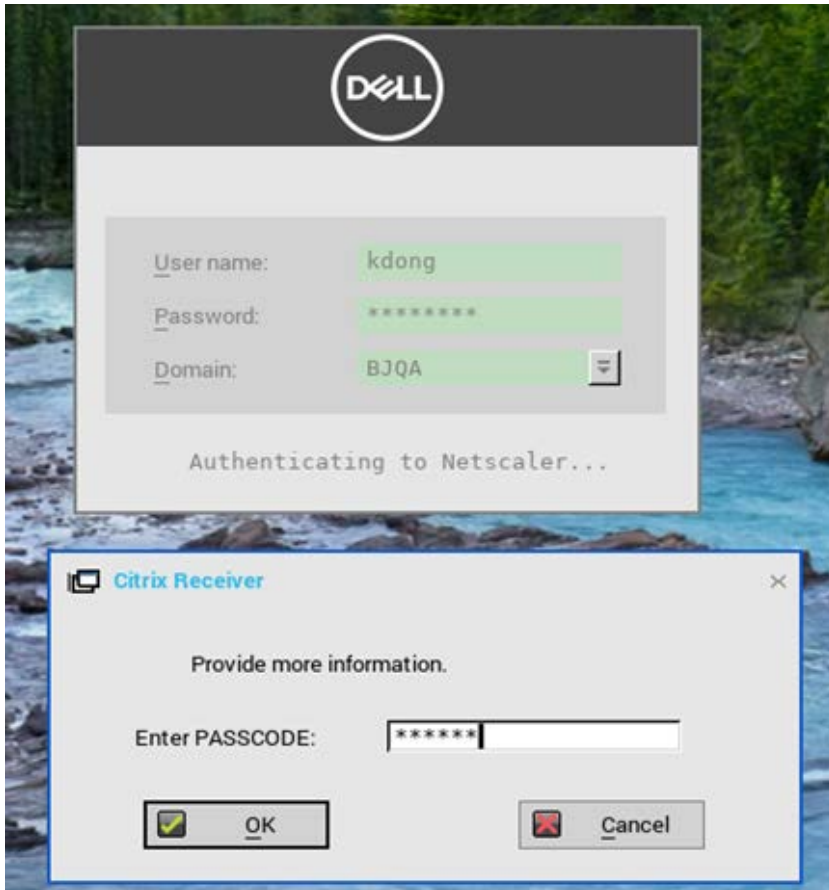
Password:

Domain: ▾

☰ CensorNet App ↻

Message

NON-TRUSTED LOCATION
PASSCODE: ihyhyw
Country: unknown
Org: ???
Dell Wyse
Message downloaded 2017/10/11 16:32:53



Citrix #3 RTME/RTOP 2.3

RTME 2.3 is included in ThinOS Lite v2.4.

Known issues / Limitations

- Citrix changed the video performance design to lower CPU consumption for other applications, and this affects the video resolution when compared to v2.2.
- RTME 2.2 PKG can be used with firmware v2.5.

Network settings change without reboot

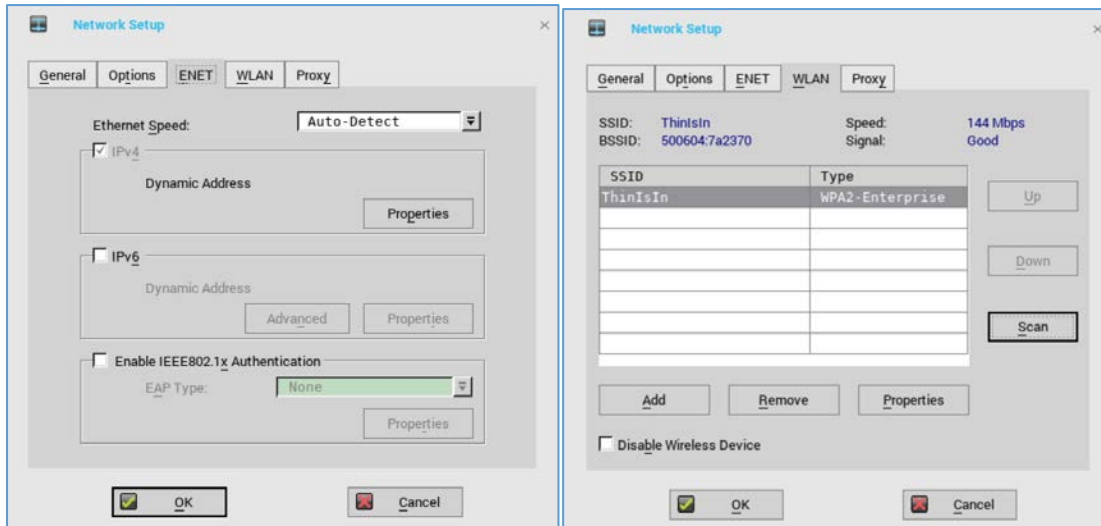
In ThinOS Lite 2.5 Lite, any change in network settings does not require reboot, all changes are applied immediately.

For example,

- Add a new wireless SSID.
- After that, ThinOS Lite connects to the wireless SSID immediately, you need not reboot.

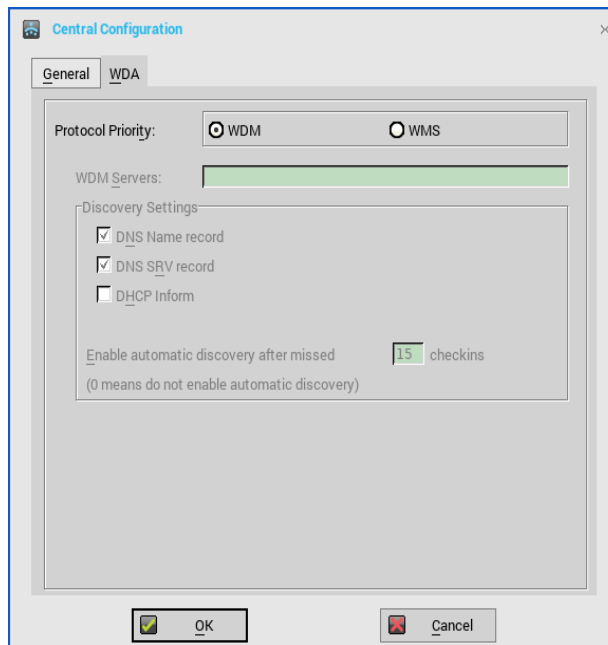
Limitation

- On ARM platforms (3010, 3020), disable/enable wireless will require system reboot.



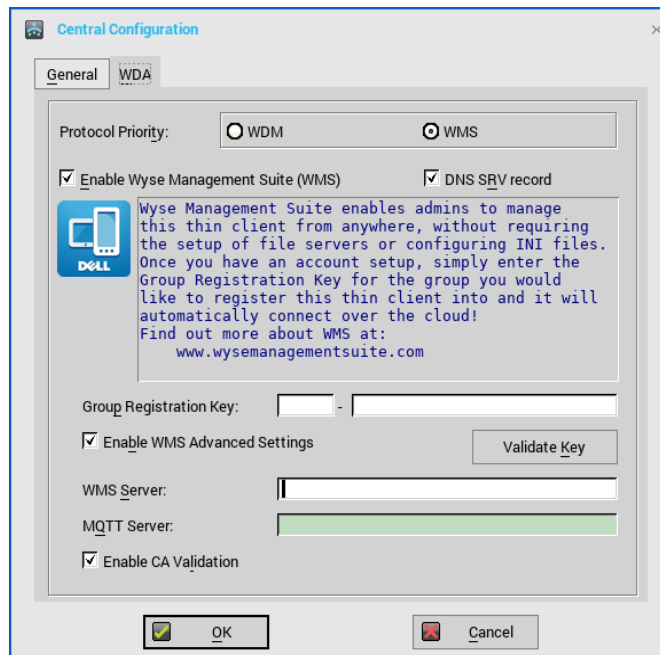
Wyse Device Manager/Wyse Management Suite changes

- In Wyse Device Manager on ThinOS Lite, Central Configuration > WDA.
 - The default protocol is changed from WDM to WMS.
 - WDM GUI can now be disabled using one of following INI parameter:
 - WDMService=no
 - Service=wdm disable=yes
 - RapportDisable=yes



What's new: Support for Wyse Management Suite v1.1. For more information, see Dell Wyse Management Suite 1.1 Administrator's Guide.

- Rebranded CCM as WMS for all related labels on UI panels, and updated related INI parameters and descriptions.



- For a private Wyse Management Suite Server, Group Registration Key is not required. You can provide Wyse Management Suite Server value to trigger Wyse Management Suite check-in. ThinOS Lite will register to quarantine tenant.
- WMS Server field—populates return value from Wyse Management Suite server after check-in.
- MQTT Server field is disabled—populates the return value from Wyse Management Suite server after check-in.
- Support all new ThinOS Lite v2.5 and later from Wyse Management Suite settings from the Group Policy tab.
 - (a) For ThinOS Lite version earlier than 2.5, configuration is not possible from Wyse Management Suite.
 - (b) In ThinOS Lite with 2.5 or later, configuration is possible from Wyse Management Suite.
 - (c) If you configure both Remote Connection and remote connection related to payload such as Broker/VDI/Connection, you need to consider the following:
 - (i) If ThinOS Lite version is 2.5 or later—remote connection is not sent from Wyse Management Suite. Remote connection related payload is sent.
 - (ii) If ThinOS Lite version is earlier than 2.5—Remote Connection is sent. Remote connection related payload is not sent.
- Support for uploading of INI file in group INI Setting payload of Group Policy in Wyse Management Suite. The priority of Wyse Management Suite INI parameter is as follows:
 - (i) INI commands in INI file has the highest priority. Other payloads from UI has the lowest priority.
 - (ii) There are three INI files after Wyse Management Suite check-in such as global group INI, group INI in user group, and device INI in device exception. The file priority is as displayed:
 1. Group INI overrides global group INI.
 2. Device INI overrides group INI and Device INI has the highest priority.

- (iii) Wyse Management Suite sends only group INI at the lowest level. For example, in the following settings in Wyse Management Suite Group Policy, the device Tom-ThinOS Lite-2.5 will receive global.ini, santaClara.ini, and Tom.ini, devices and receives global.ini and santaClara.ini from Wyse Management Suite (group INI file at the lowest level is selected based on Wyse Management Suite hierarchy).
 - Global group (INI file: global.ini)
 - USA (INI file: usa.ini)
 - CA
 - Santa Clara (INI file: santaClara.ini)
 - Tom-THINOSLite -2.5 (INI file: Tom.ini)
 - China
 - Beijing
- Support for Wyse Management Suite server function **Able to change CA validation for file repository**.
- Support Wyse Management Suite Server function **Send heartbeat and check-in interval to the agent** in ThinOS Lite.
 - (a) Whenever Wyse Management Suite agent checks-in to server, it may receive heartbeat and check-in interval if it is configured on WMS console, WMS agent should update and apply them accordingly.
 - (b) Whenever Wyse Management Suite agent send heartbeat to server, it should receive heartbeat interval and command pending flag.

Technical References

- Wyse Management Suite registration workflow example on a Public Cloud Workflow.
 - Configure ThinOS Lite with Wyse Management Suite server URL and group token registration key.
 - Device registers to Wyse Management Suite using the server URL and group token.
 - Device calls /device/ MQTT with all current authentication headers.
 - Device connects to MQTT server with the URL from /device/mqtt.
 - If device fails to connect to MQTT, event log is sent to Wyse Management Suite server with the MQTT URL and administrator can see if the firewall rule allows connection to the MQTT server/port.
- Wyse Management Suite registration workflow on a Private Cloud Workflow: Registration with server URL and group token (group registration key)
 - Configure ThinOS Lite with Wyse Management Suite server URL and group token.
 - Device registers to Wyse Management Suite using the server URL and group token.
 - Device calls /device/mqtt with all current authentication headers.
 - Device connects to MQTT server with the URL returned from /device/mqtt.
 - If device fails to connect to MQTT, event log is sent to Wyse Management Suite server with the MQTT URL and administrator can see if the firewall rule allows connection to the MQTT server/port.
- Wyse Management Suite registration workflow example on a Private Cloud Workflow: Registration with server URL only
 - Configure ThinOS Lite with Wyse Management Suite server URL.
 - Device registers to Wyse Management Suite using the server URL.
 - If there is only one tenant in the server, server returns Quarantine group's owner ID.
 - Alternatively, server returns error for the missing group token.

- Device proceeds to register with the owner ID it receives from Wyse Management Suite server.
- Device calls /device/mqtt with all current authentication headers.
- Device connects to MQTT server with the URL returned from /device/mqtt.
 - If device fails to connect to MQTT, event log is sent to Wyse Management Suite server with the MQTT URL and administrator can see if the firewall rule allows connection to the MQTT server/port.
- MQTT Validation
 - Private cloud MQTT is installed on the same server with Wyse Management Suite from 1.0 release.
 - If the agent cannot connect to MQTT, it should be the same except that it should store the MQTT URL in the event log.
 - Wyse Management Suite returns MQTT URL during JSON check-in.
 - If the agent has problem with MQTT connectivity, it needs to check if the current MQTT URL is the same as JSON check-in.
 - If it is different, agent needs to connect to the new MQTT server specified in the JSON check-in.
 - If there are any pending commands, agent should apply the required commands.
- Ability to change Wyse Management Suite and MQTT workflow
 - Agent checks in to Wyse Management Suite.
 - Agent checks for URL changes.
 - MQTT: if the current MQTT server is different from the MQTT URL, agent should attempt to switch to the new MQTT.
 - For Successful connection, agent should use the latest version of the MQTT server.
 - During failure, agent should retain the current connection and send a notification to server. (Description: Failed to connect to MQTT %mqttUrl. Current MQTT server %currentMqtt).
 - Wyse Management Suite server: if the current Wyse Management Suite server URL is different from the URL during check-in, agent should attempt to switch to the new Wyse Management Suite URL.
 - For successful connection, agent should use the new Wyse Management Suite server.
 - During failure, agent should keep the current connection, and send a notification to server. When it fails to connect to Wyse Management Suite Server %wmsUrl. Current WMS server %currentWMS.
 - Port—if Wyse Management Suite server URL does not have port detail, default port should be used. Default port for HTTP is 80. Default port for HTTPS is 443.

Troubleshooting

- ThinOS Lite devices allow secure SSL connections—SecurityMode=Full option—only after verifying if the certificates are valid. In the present scenario, the devices enforce the warning policy after you define a server using a valid IP address. The resolution for the issue will be delivered in the next ThinOS Lite release.

The following are the workarounds to avoid the SSL connection issue:

- o Ensure that the device has a valid certificate and the correct time is selected on the device.
- o Define the server by name instead of IP address.
- o Set the value of the global security policy to high.
- o Use the following INI parameter to enforce the high security mode:
`SecurityPolicy=high TLSCheckCN=Yes`
- Firmware/Package update—When the packages fail to update or cannot function (cannot connect desktop) after update with new version firmware; if there is further failure, a work around would be to remove all packages and re-install all of them on reboot.
- Boot up unit without monitor or with monitor power off.
 - o Wyse 5010 zero client with Citrix—If the client waits for 15-20 seconds and the monitor is attached or power on within 20 seconds, the display turns on. If the monitor is attached or power on occurs after 20 seconds, the monitor be in black screen. It is recommended to power on monitor first, not to power on client first and then power on monitor or attach monitor.
 - o From ThinOS Lite version 2.5, the ELO touch screen does not work in certain scenarios. Dell recommends that you use the touch screen listed in the [Tested Peripherals matrix](#).

INI parameters

The following are the INI parameters in this release:

Table 4. INI Parameters

Device=audio* [local_button=yes, no]*	local_button=[yes, no] The default option is yes. If the option no is selected, the mute, volume up and volume down buttons are disabled in ThinOS Lite local, however works during the session.																									
SessionConfig=ICA [ClientName=_client_name_]*	ClientName specifies the client name for ICA session. The default value is terminal name. A system variable can be used, for example, SessionConfig=ICA ClientName=\$mac NOTE: The mac address includes a special character '!'. The special character may cause the following issue: Etoken Java (aladdin) and Etoken CardOS SmartCard fail to logon XenDesktop 7.15 desktop.																									
ScreenSaver=value [Type={0,1,2,3,4}] [VideoLink=httpblink]* [VideoSpan=no]* [Unit=hour]*	<table border="1"> <thead> <tr> <th>Value</th> <th>Delay Before Starting</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Disabled</td> </tr> <tr> <td>1</td> <td>1 Minute</td> </tr> <tr> <td>3</td> <td>3 Minutes</td> </tr> <tr> <td>5</td> <td>5 Minutes</td> </tr> <tr> <td>10</td> <td>10 Minutes</td> </tr> <tr> <td>15</td> <td>15 Minutes</td> </tr> <tr> <td>30</td> <td>30 Minutes</td> </tr> </tbody> </table>	Value	Delay Before Starting	0	Disabled	1	1 Minute	3	3 Minutes	5	5 Minutes	10	10 Minutes	15	15 Minutes	30	30 Minutes	<p>The default screen saver value is 10 minutes and the maximum value is 180 minutes. The value can be between 0 and 180. If the value is different from the one in the table, it will be added to the drop down list in the GUI.</p> <p>The optional parameter Unit=hour converts screen saver timer value from minutes to hours to set a longer time.</p> <p>The optional parameter Type specifies which type of screen saver to use</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Type of Screen Saver</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Turn Screen Off</td> </tr> <tr> <td>1</td> <td>Flying Bubbles</td> </tr> <tr> <td>2</td> <td>Moving Image</td> </tr> </tbody> </table>	Value	Type of Screen Saver	0	Turn Screen Off	1	Flying Bubbles	2	Moving Image
Value	Delay Before Starting																									
0	Disabled																									
1	1 Minute																									
3	3 Minutes																									
5	5 Minutes																									
10	10 Minutes																									
15	15 Minutes																									
30	30 Minutes																									
Value	Type of Screen Saver																									
0	Turn Screen Off																									
1	Flying Bubbles																									
2	Moving Image																									

	<table border="1"> <tr> <td>3</td> <td>Showing Pictures</td> </tr> <tr> <td>4</td> <td>Playing Video</td> </tr> </table> <p>If type is set to 4, it will play video residing in the video link address VideoLink. The optional parameter VideoLink is to specify the video link address of video file. Http link such as http://10.151.134.43/test.mp4 is supported, and mp4 video format is supported. The optional parameter VideoSpan is to specify the video display mode in the screen. If Dual head is in span mode and VideoSpan=yes, it is spanned in all the screens. If VideoSpan=no, it is displayed in the main screen.</p>	3	Showing Pictures	4	Playing Video
3	Showing Pictures				
4	Playing Video				
\$DHCP(extra_dhcp_option)*	<p>Extra DHCP options which are for win CE unit, including 169, 140, 141, 166, 167</p> <p>For example, set a string test169 for option tag 169 in DHCP server, set TerminalName=\$DHCP(169) in xen.ini Check terminal name in GUI, the terminal name will be test169. The 166 and 167 is default for WMS MQTT Server and WMS CA Validation in ThinOS Lite. So need to remap the options from GUI or INI if want to use \$DHCP(166) and/or \$DHCP(167).</p>				
PRIVILEGE=[None, Low, High] [FastDHCP={yes,no}]*	<p>FastDHCP identifies gateway first. If the DHCP information has not expired and the connection to the network is same as the one before disconnection, the previous DHCP information is used. A new DHCP process is not started. The default value is yes.</p>				
VPN=openconnect [Username-enc=encrypted_username_string]* [Password-enc=encrypted_password_string]*	<p>The VPN configures the OpenConnect VPN session. It can allow up to 4 connections.</p> <ul style="list-style-type: none"> · The option Username-enc specifies AES encrypted login username. · The option Password-enc specifies AES encrypted login password. 				
PnLiteServer=List of {IP address, DNS names or URLs} [SFIconSortMode={0, 1, 2, 3}]*	<p>This option provides a list of host names or IP addresses with optional TCP port number or URLs of PN-Lite servers. Default value is Empty. Each entry with optional port is specified as Name-or-IP;port, where :port is optional, if the port is not specified, port 80 is used. Once specified, it is saved in the non-volatile memory. The statement PNAgentServer and NFuseServer is equal to this statement. NOTE: When Multifarm=yes, use # to separate failover servers, and use a comma or semi colon to separate servers that belong to different farms. SFIconSortMode sorts storefront dekstop icon. The default value is 0. 0— sorts by the position value from server side. 1— sorts in alphabetical order with desktop first. 3—sorts in alphabetical order with application first.</p>				
Device=cmos [AutoPowerDate={yes,no}]* [AutoPowerTime={hh:mm:ss}]* [AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]*	<p>[[AutoPowerDate={yes,no}]]</p> <p>This option is set to enable the time and day for the system to turn on automatically. If the value No is specified the system does not automatically start at the time specified in AutoPowerTime and AutoPowerDays. If the value Yes is specified the system starts at the time specified in AutoPowerTime and AutoPowerDays. [AutoPowerTime=hh:mm:ss]</p>				

	<p>This option specifies auto power on time, value range of hh is 0 - 23 while mm and ss is 0 - 59. [AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]</p> <p>This option specifies the days to turn on the system automatically. For example, Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday;Saturday</p>
Folder=[folder]*	Folder groups the connections. This option Displays the folder on ThinOS Lite desktop only if classic mode is set and signon=yes icongroupstyle=folder . The folder can include sub folder.
Device=cmos [CurrentPassword= password NewPassword = password] *	[CurrentPassword= password NewPassword = password] This option is used to change the device BIOS password. CurrentPassword is required. The maximum count of password string is 19 bytes.

NOTE: INI parameter with an asterisk is a newly added parameter.

Fixed issues

Table 5. Fixed issues

Sl.No	Issues
1	Improvements in Citrix Receiver logo display quality when using light desktop background colors
2	Extended the screensaver activation period, but adding an option to convert defined units from minutes to hours
3	Added OKTA authentication for PCoIP connections
4	Addressed and issue preventing the mouse over effect from showing application farm information
5	Added support for Entrust multifactor authentication
6	Added 1720x1440 desktop resolution support
7	Added the ability to organize RDP desktop icons into folders
8	Added support for ATOS CardOS broker authentication
9	The full path of file server is now shown in the user interface
10	Added support for Hitachi Biometric reader with smartcard (P/N PC-KCB110)
11	Added support for video screensavers
12	DHCP option 199 for Wyse Management Suite causes factory reset with 2.5 firmware

Test environment

The following reference table is for the tested server versions for this release. This is not the environment support matrix. The supported versions are not limited to the tested versions. ThinOS Lite is compatible with both earlier and current server versions.

Table 6. Tested environment

Application	Version
WMS	1.1
WDM	5.7.2
Imprivata	5.2.0.15
Caradigm	6.5.1
Netscaler	9.3/10.0/10.1/10.5/11.0/11.1/12.0
Storefront	3.6/3.11
Web Interface	5.4
SecureMatrix	4.1.0

Application	Windows 7	Windows 8.1	Windows 10	Linux	Windows 2008 R2	Windows 2012 R2	Windows 2016	APPs
XD 5.6	Yes	No	No	No	No	No	No	No
XA 6.5	No	No	No	No	Yes	No	No	Yes
XD/XA 7.6	Yes	Yes	No	Yes	Yes	Yes	No	Yes
XD/XA 7.15	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes

XD/XA	OS	RTME	Lync client	Lync server	SFB server
7.6	Windows 8.1	1.8	Lync 2013	Lync 2013	NA
7.6	Windows 2012 R2	2.3	SFB 2015	NA	SFB 2015
7.15	Windows 7	2.3	SFB 2016	NA	SFB 2015
7.15	Windows 10	2.3	SFB 2016	NA	SFB 2015
7.15	Windows 8.1	2.3	SFB 2016	NA	SFB 2015
7.15	Windows 2016	2.3	SFB 2016	NA	SFB 2015

Tested peripherals

Described below are the tested devices for the release. This is not the peripherals/device support list. The supported devices are not limited to the tested devices. The following table lists the tested peripherals:

Table 7. Tested peripherals

Device	Model
Audio	Jabra Pro 935 MS Wireless headset (Mono) - Office Centric
Cables	Dell DP to HDMI Adapter
Cables	Dell DP to VGA Adapter
Input Devices	Dell Wireless Keyboard and mouse combo (KM636)
Input Devices	Dell USB Wired Keyboard - KB216
Input Devices	DellUSB Wired Optical Mouse - MS116
Input Devices	Dell USB Wired Keyboard with Smart Card reader - KB813
Monitors	Dell 19 Monitor - E1916H
Monitors	Dell 20 Monitor - E2016

Monitors	Dell 20 Monitor - E2016H
Monitors	Dell 20 Monitor - E2316H
Monitors	Dell 20 Monitor - P1917S
Monitors	Dell 20 Monitor - P2016
Monitors	Dell 20 Monitor - P2017H
Monitors	Dell 22 Monitor - P2217H with stand
Monitors	Dell 22 Monitor - E2216H
Monitors	Dell 23 Monitor - P2317H
Monitors	Dell 23 Monitor - P2717H
Monitors	Dell 23 Monitor- E2318H
Monitors	Dell 24 Monitor - E2417H
Monitors	Dell 24 Monitor - P2417H with stand
Monitors	Dell 24 Monitor - U2415

Table 8. Tested peripherals

Peripheral Name	Type
Dell E2416Hb (1920x1080)	Monitor
Dell E2715Hf (1920x1080)	Monitor
Dell UP3216Qt(3480X2160)	Monitor
Dell P2415Q(3480X2160)	Monitor
Dell P2714Hc (1920x1080)	Monitor
Dell P2715Q(3840x2160)	Monitor
Dell P2815Qf (3840x2160)	Monitor
Dell U2713Hb (2560x1440)	Monitor
Dell U2713HM (2560x1440)	Monitor
Dell U2713HMT (2560x1440)	Monitor
Dell U2718Qb (3840x2160)	Monitor
Dell U2718Q (3480X2160)	Monitor
Dell U2913 WM (2560x1080)	Monitor
Dell U3014t (2560x1600)	Monitor
Dell S2817Q(3840x2160)	Monitor
Dell UZ2315H (1920x1080)	Monitor
Dell 3008WFP (2560x1600)	Monitor
Dell P2418HT(1920x1080)	Touch Screen
Dell B1163 Mono Multifunction Printer	Printer
Dell B1165nfw Mono Multifunction Printer	Printer
Dell B1260dn Laser Printer	Printer
Dell B1265dnf Multifunction Laser Printer	Printer
Dell B2360d Laser Printer	Printer
Dell B2360dn Laser Printer	Printer
Dell B2375dnf Mono Laser Multifunction Printer	Printer
HP LaserJet P2055d	Printer
HP LaserJet P2035	Printer

Peripheral Name	Type
HP LaserJet 1022n	Printer
HP Color LaserJet CM1312MFP	Printer
EPSON PLQ-20K	Printer
Dell KM636 Wireless Keyboard and Mouse	Keyboard/mouse
DELL wireless Keyboard/mouse KM632	Keyboard/mouse
DELL wireless Keyboard/mouse KM714	Keyboard/mouse
Dell Keyboard KB212-B	Keyboard/mouse
Dell Keyboard KB216p	Keyboard/mouse
Dell Mouse MS111-P	Keyboard/mouse
Dell Mouse MS116-P	Keyboard/mouse
Dell Keyboard SK-3205 (Smartcard reader)	Keyboard/mouse
Dell Optical Wireless Mouse – WM123	Keyboard/mouse
Dell Wireless Mouse – WM324	Keyboard/mouse
Dell Wireless Bluetooth Travel Mouse – WM524	Keyboard/mouse
Logitech K480 Keyboard, Bluetooth	Keyboard/mouse
Logitech K400 Plus	Keyboard/mouse
Logitech M557 mouse, Bluetooth	Keyboard/mouse
Microsoft Arc Touch Mouse 1428	Keyboard/mouse
Microsoft ARC touch mouse 1592, Bluetooth	Keyboard/mouse
Microsoft Designer Bluetooth Keyboard/Mouse	Keyboard/mouse
Rapoo E6100, Bluetooth	Keyboard/mouse
Cherry RS 6700 USB (Smartcard reader)	Keyboard/mouse
SpaceNavigator 3D Space Mouse	Keyboard/mouse
Jabra PRO 935 MS	USB Headset
Jabra PRO 9450	USB Headset
Jabra PRO 9470, Bluetooth	USB Headset
Jabra Speak 510 MS, Bluetooth	USB Headset
Jabra Evolve 75	USB Headset
Jabra Evolve 40 MS Mono	USB Headset
Jabra UC SUPREME MS /LINK 360, Bluetooth	USB Headset
Jabra UC Voice 550 MS Duo	USB Headset
Jabra GN2000	USB Headset
Plantronics BLACKWIRE C420	USB Headset
Plantronics BLACKWIRE C520	USB Headset
Plantronics SAVI W740/Savi W745	USB Headset
Plantronics SAVI W740 3IN1 Convertible, UC, DECT 6.0 NA, Bluetooth	USB Headset
Plantronics SAVI List 400 series	USB Headset
Plantronics Voyager Legend UC B235 NA, Bluetooth	USB Headset
Plantronics Calisto P240 D1K3 USB handset	USB Headset
Plantronics Calisto 620-M, Bluetooth	USB Headset
Plantronics DA60	USB Headset
Plantronics P420	USB Headset
Plantronics USB DSP DA40(B)	USB Headset

Peripheral Name	Type
SENNHEISER USB SC230	USB Headset
SENNHEISER SP 20 ML Speakerphone for Lync and mobile devices	USB Headset
SENNHEISER SC 660 Binaural CC&O HS, ED	USB Headset
SENNHEISER SC 260 USB MS II	USB Headset
SENNHEISER SP 10 ML Speakerphone for Lync	USB Headset
SENNHEISER D 10 USB ML-US Wireless DECT Headset	USB Headset
SENNHEISER DW Pro2 ML	USB Headset
SENNHEISER SC 75 USB MS	USB Headset
SENNHEISER MB Pro 2 UC ML	USB Headset
POLYCOM Deskphone CX300	USB Headset
LFH3610/00 SPEECHMIKE PREMIUM	SPEECHMIKE PREMIUM
LFH3200/00 SPEECHMIKE PREMIUM	SPEECHMIKE PREMIUM
LFH3210/00 SPEECHMIKE PREMIUM	SPEECHMIKE PREMIUM
Dell USB Soundbar AC511	Audio soundbar
Logitech C525 HD Webcam	USB Webcam
Logitech C920 HD Pro Webcam	USB Webcam
Logitech C930e HD Webcam	USB Webcam
Logitech BCC950 ConferenceCam	USB Webcam
Logitech USB Webcam 9000	USB Webcam
Logitech ConferenceCam CC3000e	USB Webcam
Microsoft LifeCam 3.0 Cinema	USB Webcam
Microsoft LifeCam HD-3000	USB Webcam
SanDisk USB 3.0 16GB	Data storage
SanDisk Extreme USB 3.0 16G	Data storage
Kingston DataTraveler 100 G3	Data storage
Kingston DataTraveler G3 16GB	Data storage
Kingston DataTraveler G3 8GB	Data storage
Kingston DataTraveler Elite 3.0 16G	Data storage
Kingston DTM30 32GB	Data storage
ADATA S107/16GB	Data storage
ADATA S102/16GB	Data storage
ADATA UV150 USB 3.0 16GB	Data storage
BENQ DVD Drive	USB DVD RW
SAMSUNG PorTable DVD Writer SE-208	USB DVD RW
Dell SW316	USB DVD RW
HTC one-XL	Mobile Phone
iPhone 7	Mobile Phone
Samsung Galaxy 7	Mobile Phone
DP-DVI Convertor	Converter Display
DP-VGA Convertor	Converter Display
Dell DP-VGA convertor	Converter Display
Dell DP-DVI KKMYPD convertor	Converter Display
Cisco GLC-T 30-1410-03 B2 V03	Converter Network
TRANSITION SGFEB 1040-120	Converter Network
Prolific USB-to-Serial converter U232-P9V2	Converter USB

Peripheral Name	Type
USB-to-Serial converter	Converter USB
Dell Keyboard M/N KB813	Smartcard Reader
Dell Keyboard SK-3205	Smartcard Reader
Cherry keyboard RS 6600	Smartcard Reader
Cherry keyboard RS 6700	Smartcard Reader
Cherry keyboard KC 1000 SC	Smartcard Reader
Gemalto IDBridge CT710	Smartcard Reader
OMNIKEY OK CardMan3121	Smartcard Reader
HID OMNIKEY 3021	Smartcard Reader
HID OMNIKEY 5125	Smartcard Reader
HID OMNIKEY 5421	Smartcard Reader
HID OMNIKEY 5325 CL	Smartcard Reader
SmartOS powered SCR335	Smartcard Reader
Actividentity USB reader 2.0	Smartcard Reader
RDR-80581AKU	Proximity Card Reader
RDR-80582AKU	Proximity Card Reader
RDR-6082AKU	Proximity Card Reader
OMNIKEY 5025 CL	Proximity Card Reader
OMNIKEY 5326 DFR	Proximity Card Reader
OMNIKEY 5427 CK	Proximity Card Reader
OMNIKEY 5125	Proximity/Smartcard Reader
OMNIKEY 5325 CL	Proximity/Smartcard Reader
Finger Print Keyboard ET710	Fingerprint Reader
Oberthur ID One 128 v5.5	Smartcard CAC
G&D FIPS 201 SCE 3.2	Smartcard CAC
Gemalto TOPDLGX4 144	Smartcard
SafeNet SC650	Smartcard SiPR

Smart Card info from ThinOS Lite event log	Driver	Provider (CSP)	Card type
Actividentity V1	ActivClient 6.2	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
Actividentity V1 (IDClassic 230)	ActivClient 6.2	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
Actividentity V2	ActivClient 6.2	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
Gemalto/IDPrime.NET (Gemalto .net 510)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	Axalto Cryptoflex.NET(V7.2.1.0)
ID Prime MD v 4.0.2 (Gemalto 840)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.3.2.11)
ID Prime MD v 4.1.0 (Gemalto 3810)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.4.0.7)

ID Prime MD v 4.1.1 (Gemalto 830)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.4.1.7)
ID Prime MD v 4.3.5 (Gemalto 830)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.6.5.4)
Etoken CardOS	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	Siemens CardOS V4.2B
Etoken CardOS (white USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	Siemens CardOS V4.2
Etoken Java(aladdin)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	eToken PRO Java SC 72K OS755
Etoken Java(aladdin) (blue USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	eToken PRO Java 72K OS755
Etoken Java(aladdin) (black USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java(aladdin) (black USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	SafeNet eToken 5110
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	G&D STARCOS 3.0 T=0/1 0V300
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2
PIV (Yubico) (black USB key)	YubiKey PIV Manager	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_6.1.6	cv act sc/interface CSP	G&D STARCOS 3.2