Dell Wyse ThinOS 8.5_009

Release Notes

Current Version: 8.5_009
Release Date: 2018-02
Previous Version: 8.4

Contents

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 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 8.5_009

Previous version

ThinOS 8.4

Platform information

The following table lists the supported platforms and associated firmware in this release:

Platform	ThinOS	ThinOS with PCoIP
Wyse 3040 thin client	A10Q_wnos	PA10Q_wnos
Wyse 5060 thin client	D10Q_wnos	PD10Q_wnos
Wyse 5010 thin client	ZD10_wnos	PD10_wnos
Wyse 3030 LT thin client	U10_wnos	PU10_wnos
Wyse 3020 thin client	T10D_wnos	NA
Wyse 3010 thin client	DOVE_boot	NA
Wyse 5040 AIO thin client	ZD10_wnos	PD10_wnos
Wyse 7010 thin client	ZD10_wnos	NA

BIOS information

The following table lists the BIOS information in this release:

Platform	BIOS version
Wyse 3040 thin client	1.2.3
Wyse 5060 thin client	1.0 G
Wyse 5010 thin client	3.0 U
Wyse 3030 LT thin client	1.0 F
Wyse 3020 thin client	w-loader 7.0_216
Wyse 3010 thin client	EC 3.02
Wyse 5040 AIO thin client	3.0 U
Wyse 7010 thin client	3.0 U

New features

This section contains the new features and feature matrix details.

New features / platform matrix

The following table lists the new features and platforms in this release:

New Feature or Platform Matrix	**5010 ThinOS (D10D)**	**3030 LT ThinOS**	**3040 ThinOS**	**5060 ThinOS**	**3010 ThinOS (T10)**	**3020 ThinOS (T10D)**	**5040 ThinOS (5212 AIO)**	**7010 ThinOS (Z10D)**
	5010 PCoIP (D10DP)	**3030 LT PCoIP**	**3040 PCoIP**	**5060 PCoIP**			**5040 PCoIP (5213 AIO)**	
Package update	Yes	Yes	Yes	Yes	Base pkg only	Base pkg only	Yes	Yes
BIOS update	3.0U	1.0F	1.2.3	1.0G	No update	No update	3.0U	3.0U
GUI #1 First Boot Wizard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GUI #2 Zero Theme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GUI #3 Wallpaper added	Yes	Yes	Yes	Yes	No update	Yes	Yes	Yes
GUI #4 Sys Information	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GUI #5 Trouble Shooting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VMWare #1 Blast Extreme H.264	No Support	Yes	Yes	Yes	N/A	N/A	No Support	No Support
VMWare #2 Blast UDP / BEAT	Yes	Yes	Yes	Yes	N/A	N/A	Yes	Yes
VMWare #3 Broker Logon Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix #1 Multiple Audio	Yes	Yes	Yes	Yes	N/A	N/A	Yes	Yes
Citrix #2 NetScaler + SMS PASSCODE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RDP #1 WebSocket	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RDP #2 H.264 AVC444	Yes	Yes	Yes	Yes	N/A	N/A	Yes	Yes
DP Audio	No Support	Yes	Yes	Yes	N/A	N/A	No Support	No Support
Network Setting without reboot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

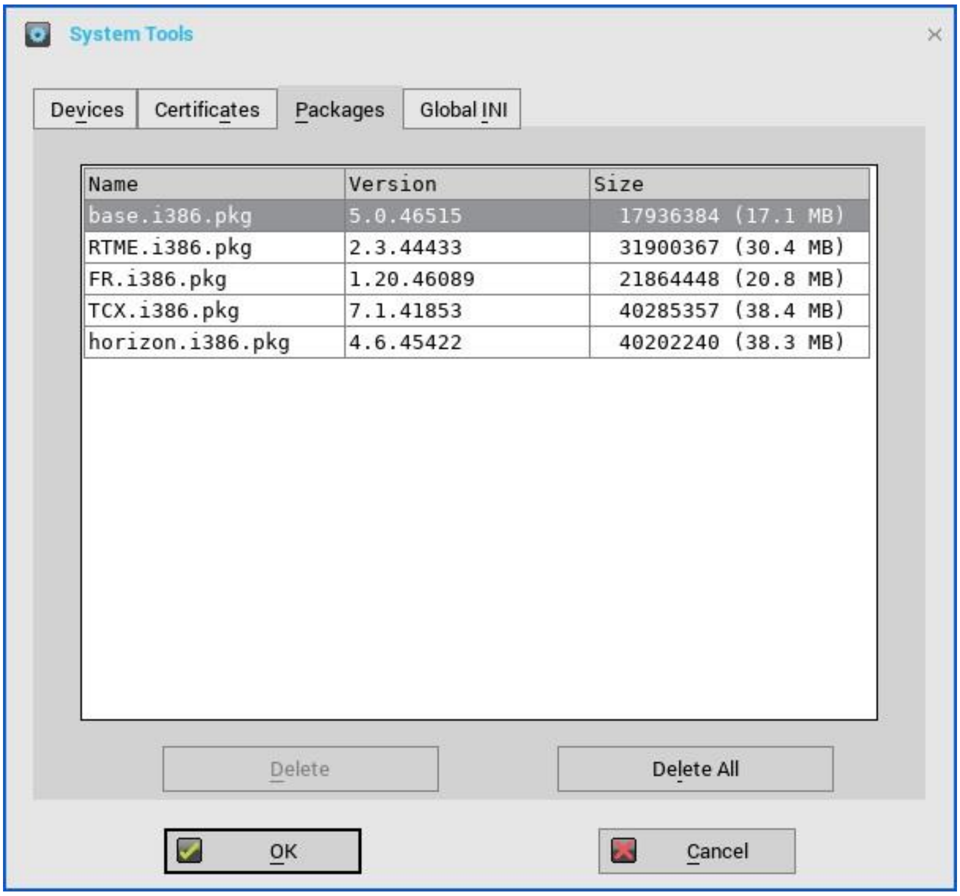
WDM/WMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Package update details

This section contains package update details.

- Packages that will auto update following firmware update. No manual effort is needed.
  - Base.i386.pkg: updated to 5.0.46515 for new firmware version
  - Pcoip.i386.pkg: no major update remain 2.9.45162
- Packages that will self-install/update without need of INI configuration. You must upload the package to the file server directory /wnos/pkg/.
  - RTME.i386.pkg: updated to 2.3.44433 following RTOP 2.3 from 8.4_110
- Packages that require INI configuration to install/update.
  - Horizon.i386.pkg: updated to 4.6.45422 following Horizon server 7.3/ client 4.6 release
  - FR.i386.pkg: updated to 1.20.46089 to resolve any issue
  - TCX.i386.pkg: no major update; version remains 7.1.41853

NOTE: Suffix version number is for ThinOS reference and has no reference with server software/application versions.



Name	Version	Size
base.i386.pkg	5.0.46515	17936384 (17.1 MB)
RTME.i386.pkg	2.3.44433	31900367 (30.4 MB)
FR.i386.pkg	1.20.46089	21864448 (20.8 MB)
TCX.i386.pkg	7.1.41853	40285357 (38.4 MB)
horizon.i386.pkg	4.6.45422	40202240 (38.3 MB)

BIOS update details

This section contains the BIOS update details.

- New BIOS fixed issues

    - System beep issue, password token support, unexpected boot issue, and so on (for Wyse BIOS).
- To make BIOS management consistent between Wyse and Dell BIOS, new INI parameter 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]
- To make BIOS management consistent between Wyse and Dell BIOS, as well as other requirements, new INI parameters are added in “Device=DellCmos” for Dell BIOS.
    1. [USBBootSupport={yes, no}]
    2. [PXEBootSupport={yes, no}]
    3. [WakeOnUSB={yes, no}]
    4. [Action={extract, restore}]
- For BIOS configuration, if the password is configured, to update any settings, the password is required to be supplied. For example, the INI parameter to update settings must be followed with “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/ Wyse 5040 thin client/ Wyse 7010 thin client/Wyse 5060 thin client/Wyse 3030 LT 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:

Requirement	**INI for BIOS management**	**Wyse 5010 thin client/Wyse 5040 thin client/Wyse 7010 thin client**	**Wyse 5060 thin client**	**Wyse 3030 LT thin client**	**Wyse 3040 thin client**
		3.0U	1.0G	1.0 F	1.2.3
Power on without beeps	N/A	Yes	Yes	Yes	Yes
Update BIOS from file server	N/A	Yes	To support post 8.5	To support post 8.5	Yes

Change BIOS password with INI	Device=DellCmos CurrentPassword={} NewPassword={}
	Device=Cmos CurrentPassword={} NewPassword={}
		Yes	Yes	Yes	Yes

Change boot order with INI	Device=cmos BootOrder={PXE, HardDisk, USB}	Yes	Yes	Yes	Not applicable

Enable/Disable PXE imaging with INI	Device=DellCmos PXEBootSupport={yes, no}	Not applicable	Not applicable	Not applicable	Yes

Enable/Disable USB imaging with INI	Device=cmos BootFromUSB={yes, no}
	Device=DellCmos USBBootSupport={yes, no}
		Yes	Yes	Yes	Yes

Manage **AC recovery** with INI	Device=cmos AutoPower={yes, no}
	Device=DellCmos ACRecovery={PowerOff, PowerOn, LastState}
		Yes	Yes	Yes	Yes

Manage **auto on time** with INI	Device=DellCmos AutoPower={Disable, Daily, Workday} AutoPowerTime=hh:mm Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday	Yes	Yes	Yes	Yes

CMOS Extract and Restore	Device=cmos Action={extract, restore} CurrentPassword={}
	Device=DellCmos Action={extract, restore} CurrentPassword={}
		Yes	Yes	Yes	Yes

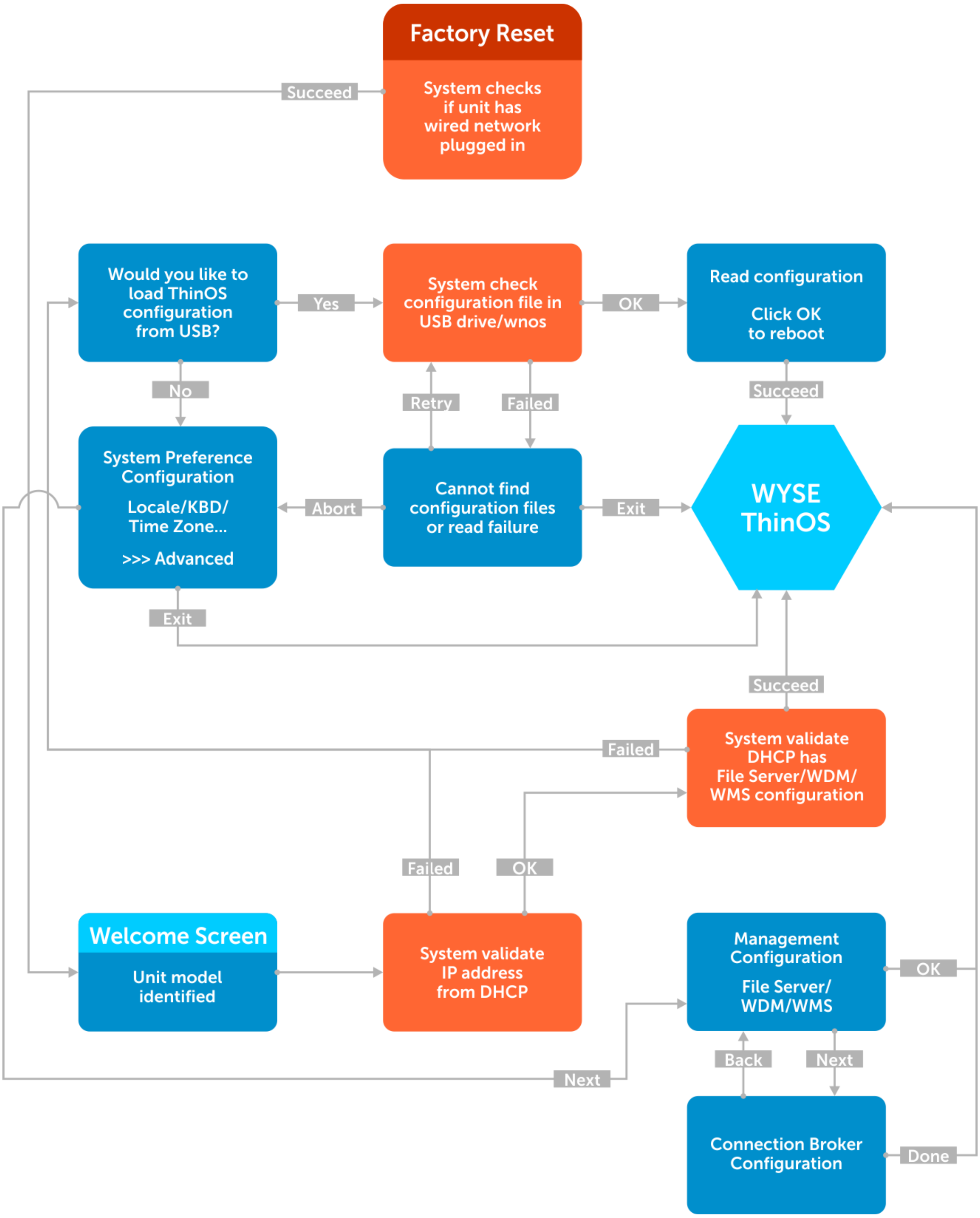
Audio management with INI	Device=cmos OnboardAudio={yes, no}
	Device=DellCmos Audio={yes, no}
		Yes	Yes	Yes	Yes

USB Port management with INI	Device=cmos USBController={yes, no} Device=DellCmos USBRearPort={yes, no} USBFrontPort={yes, no} (* Rear/Front for Dell BIOS only)	Yes	Yes	Yes	Yes
Admin lockup management with INI	Device=DellCmos AdminLock= {yes, no}	Not applicable	Not applicable	Not applicable	Yes
Wake on USB support	Device=DellCmos WakeOnUSB={yes, no}	Not applicable	Not applicable	Not applicable	Yes

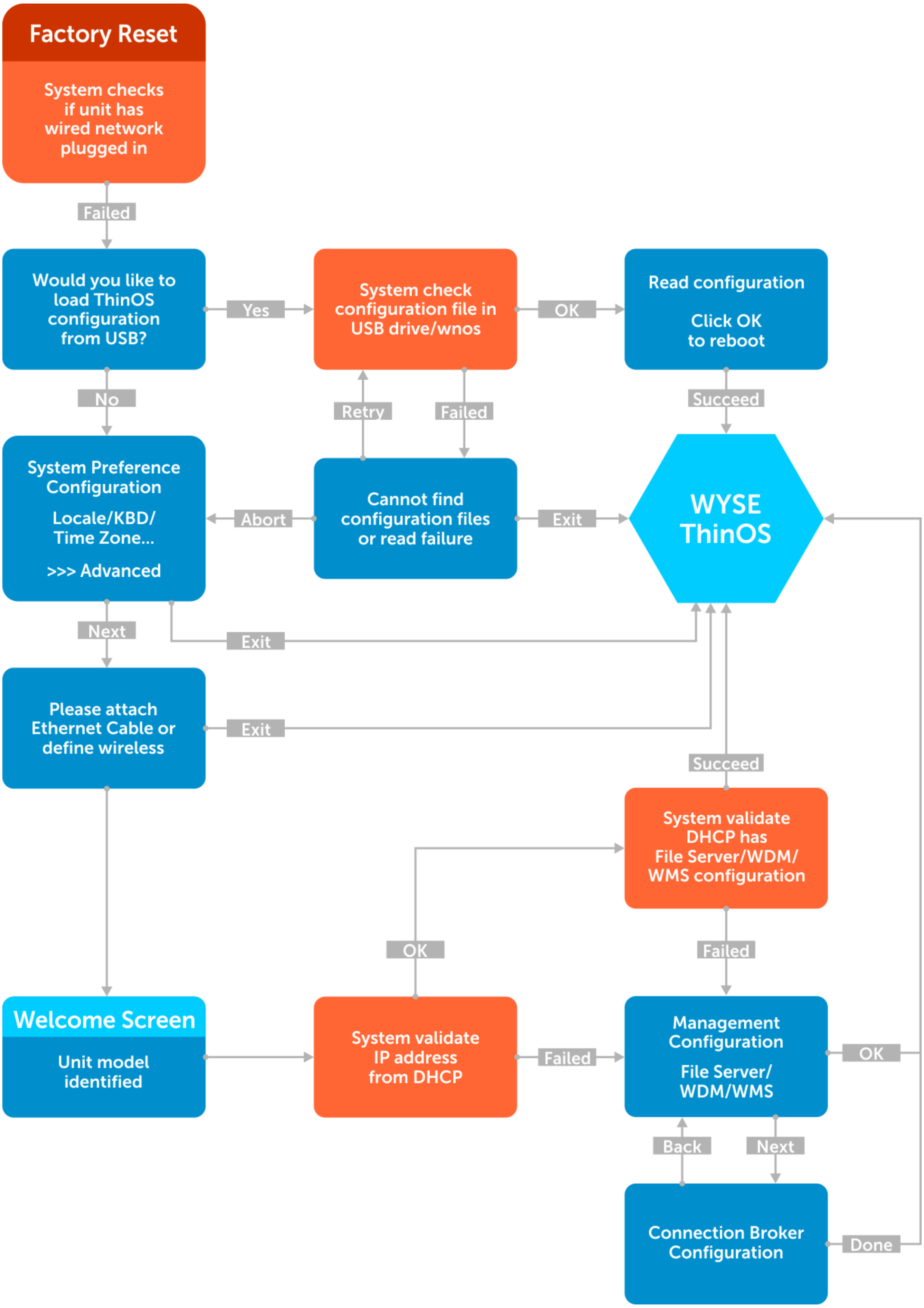
Wake On LAN	Device=cmos WakeOnLan= {yes, no}
	Device=DellCmos WakeOnLan= {Disable, LAN, PXE}
		Yes	Yes	Yes	Yes

GUI #1 First Boot Wizard

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



Factory Reset
System checks if unit has wired network plugged in
Succeed
Would you like to load ThinOS configuration from USB?
Yes
System check configuration file in USB drive/wnos
OK
Read configuration
Click OK to reboot
No
Retry
Failed
Succeed
System Preference Configuration
Locale/KBD/ Time Zone...
>>> Advanced
Abort
Cannot find configuration files or read failure
Exit
WYSE ThinOS
Exit
Succeed
Failed
System validate DHCP has File Server/WDM/ WMS configuration
Failed
OK
Welcome Screen
Unit model identified
System validate IP address from DHCP
Management Configuration
File Server/ WDM/WMS
OK
Back
Next
Next
Connection Broker Configuration
Done


Factory Reset
System checks if unit has wired network plugged in
Failed
Would you like to load ThinOS configuration from USB?
Yes
System check configuration file in USB drive/wnos
OK
Read configuration
Click OK to reboot
No
Retry
Failed
Succeed
System Preference Configuration
Locale/KBD/ Time Zone...
>>> Advanced
Abort
Cannot find configuration files or read failure
Exit
WYSE ThinOS
Next
Exit
Please attach Ethernet Cable or define wireless
Exit
Succeed
System validate DHCP has File Server/WDM/ WMS configuration
OK
Failed
Welcome Screen
Unit model identified
System validate IP address from DHCP
Failed
Management Configuration
File Server/ WDM/WMS
OK
Back
Next
Connection Broker Configuration
Done

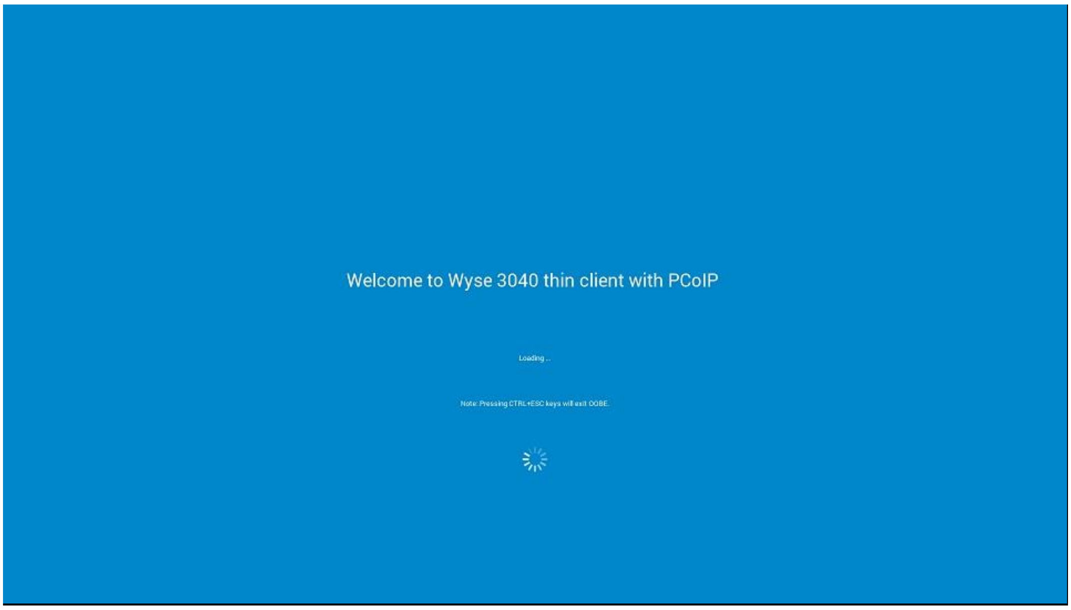
To exit First Boot Wizard

To exit First Boot Wizard, follow these steps:

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

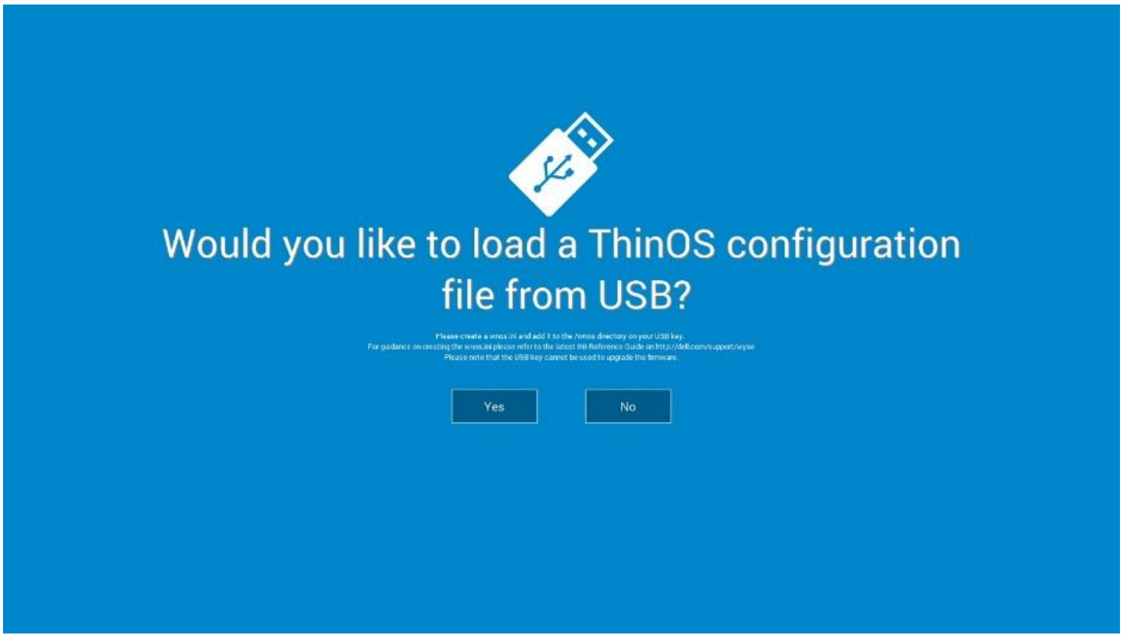


Welcome to Wyse 3040 thin client with PCoIP

Loading ...

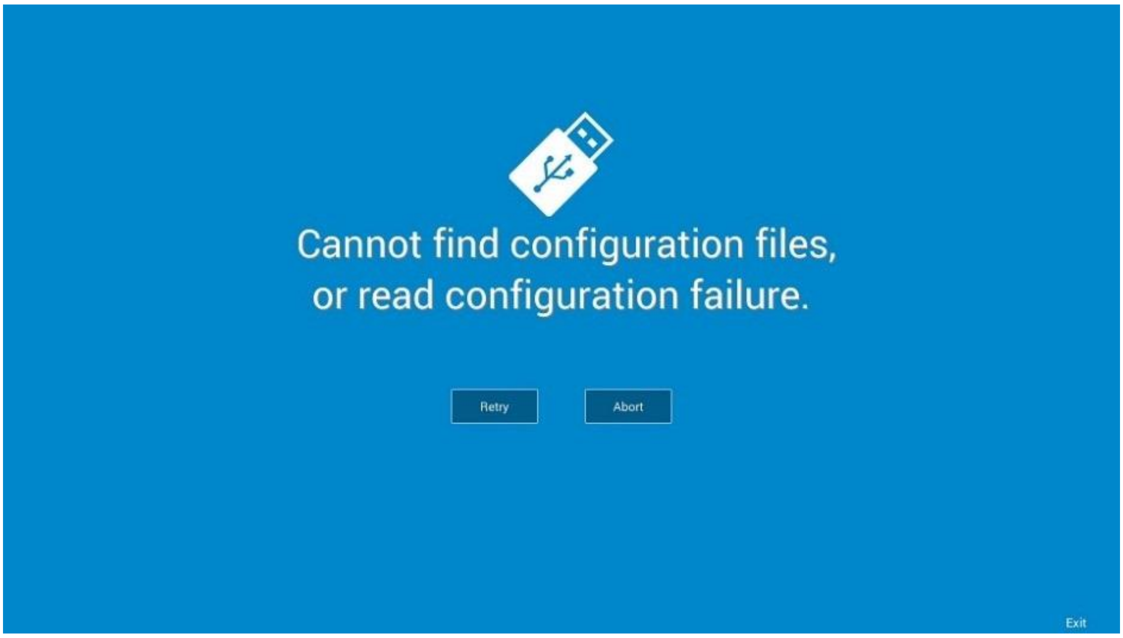
Note: Pressing CTRL+ESC keys will exit OOBE.

- Loading the USB configuration searches for configuration files such as wnos.ini and so on in USB /wnos directory.
    - All configuration files can be loaded except for firmware and package update



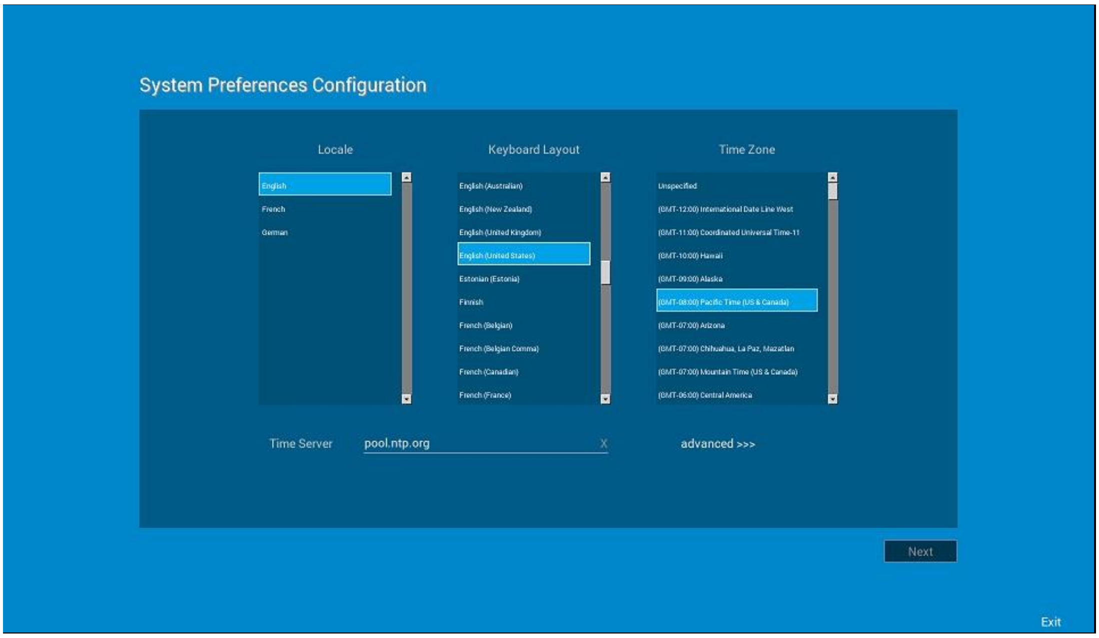
Would you like to load a ThinOS configuration file from USB?

Please create a wnos.ini and add it to the /wnos directory on your USB key.
For guidance on creating the wnos.ini please refer to the latest INI Reference Guide on http://dell.com/support/wyse
Please note that the USB key cannot be used to upgrade the firmware.



Cannot find configuration files, or read configuration failure.

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



System Preferences Configuration

Locale

- English
- French
- German

Keyboard Layout

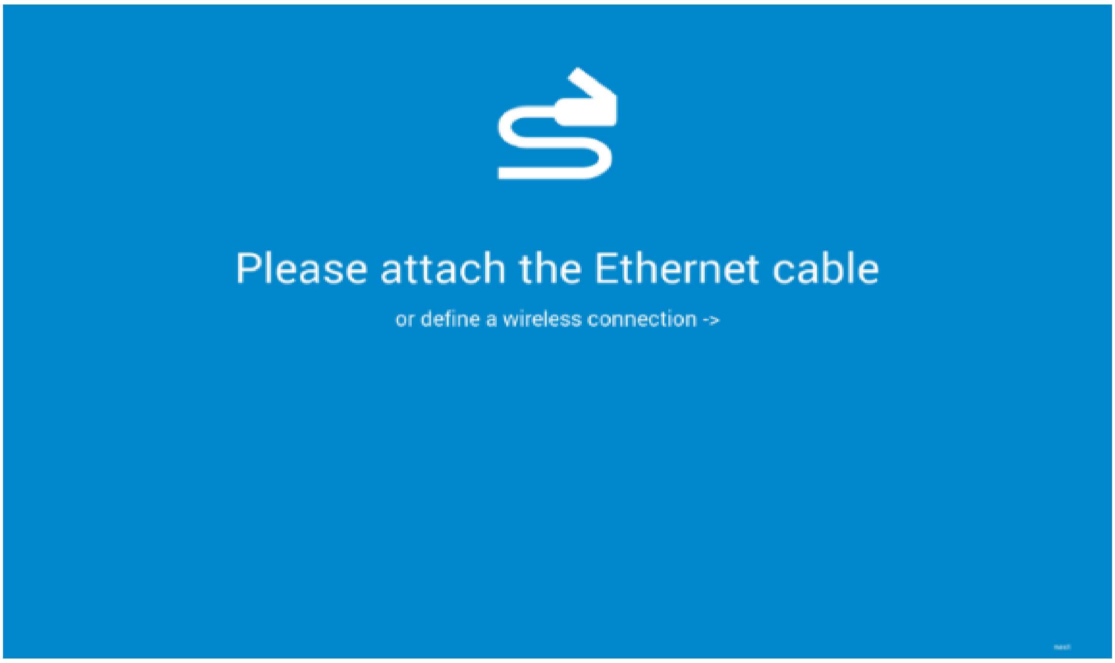
- English (Australian)
- English (New Zealand)
- English (United Kingdom)
- English (United States)
- Estonian (Estonia)
- Finnish
- French (Belgian)
- French (Belgian Comma)
- French (Canadian)
- French (France)

Time Zone

- Unspecified
- (GMT-12:00) International Date Line West
- (GMT-11:00) Coordinated Universal Time-11
- (GMT-10:00) Hawaii
- (GMT-09:00) Alaska
- (GMT-08:00) Pacific Time (US & Canada)
- (GMT-07:00) Arizona
- (GMT-07:00) Chihuahua, La Paz, Mazatlan
- (GMT-07:00) Mountain Time (US & Canada)
- (GMT-06:00) Central America

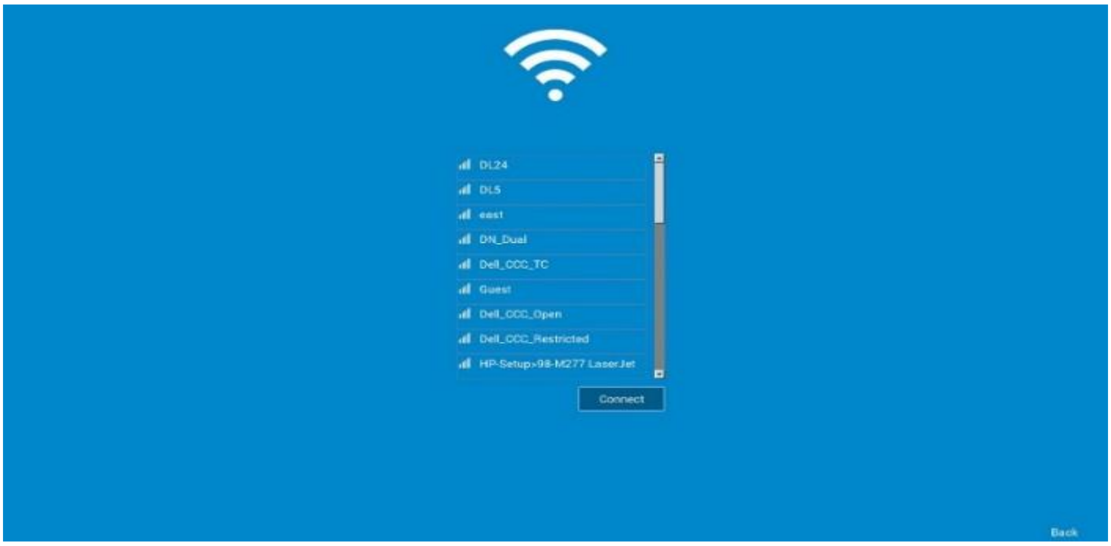
Time Server: pool.ntp.org

- 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.



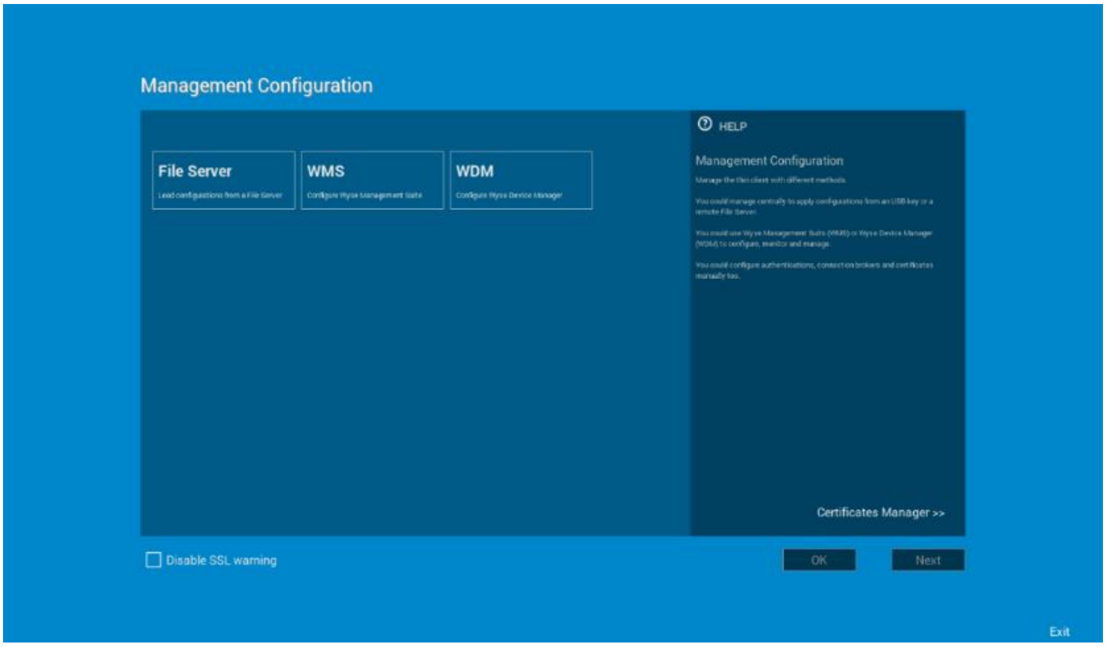
Please attach the Ethernet cable

or define a wireless connection ->



- Management Configuration—File Server, WDM, WMS
    - Additional options such as **Certificate Manager** and **Disable SSL warning** are available.
    - Finish configuration using any of the following three 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.


Management Configuration
File Server
Load configurations from a File Server
WMS
Configure Wyse Management Suite
WDM
Configure Wyse Device Manager
HELP

Management Configuration

Manage the thin client with different methods.

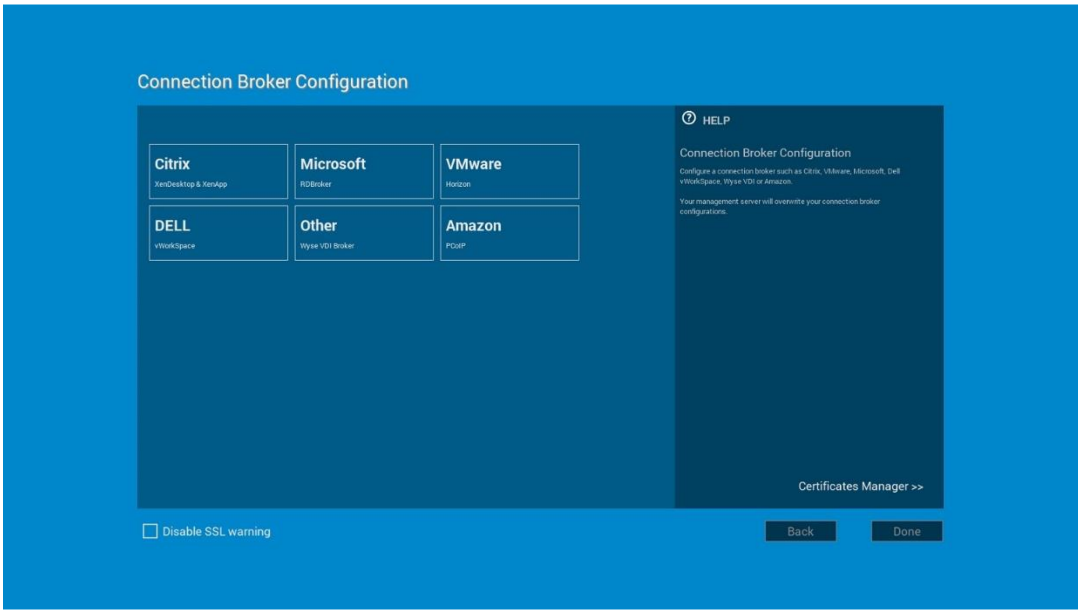
You could manage centrally to apply configurations from an USB key or a remote File Server.

You could use Wyse Management Suite (WMS) or Wyse Device Manager (WDM) to configure, monitor and manage.

You could configure authentications, connection brokers and certificates manually too.

- Connection Broker Configuration
    - Additional options such as **Certificate Manager** and **Disable SSL** warning are present
    - ThinOS options are **Citrix**, **Microsoft**, **VMware**, **DELL**, and **Others**.

- ThinOS with PCoIP options are **Citrix**, **Microsoft**, **VMware**, **DELL**, **Other**, **Amazon.**



Connection Broker Configuration

HELP

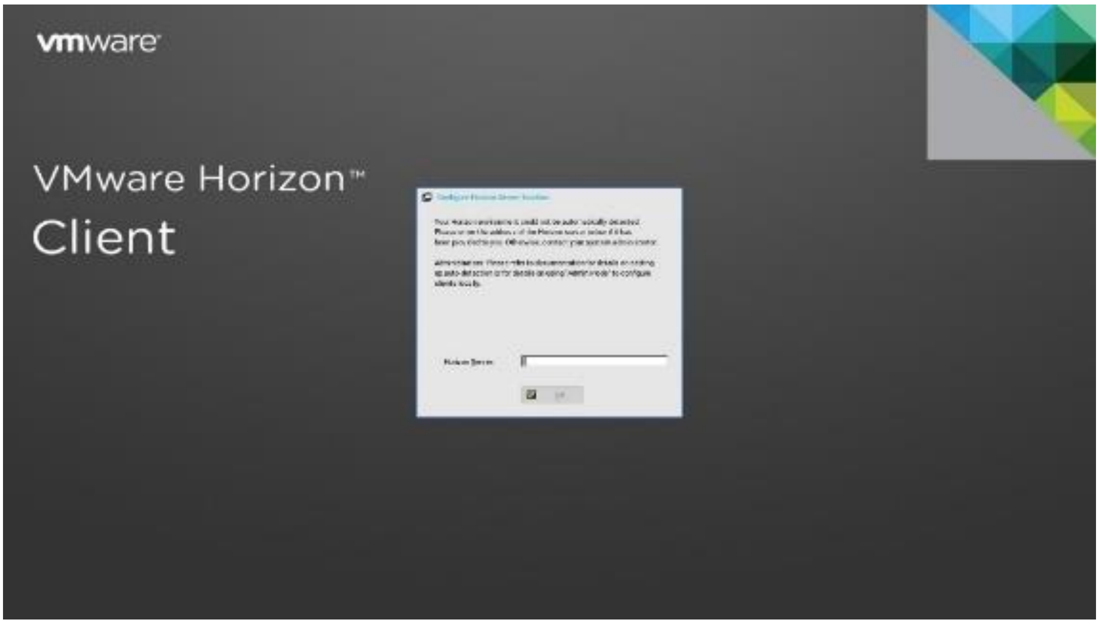
Connection Broker Configuration

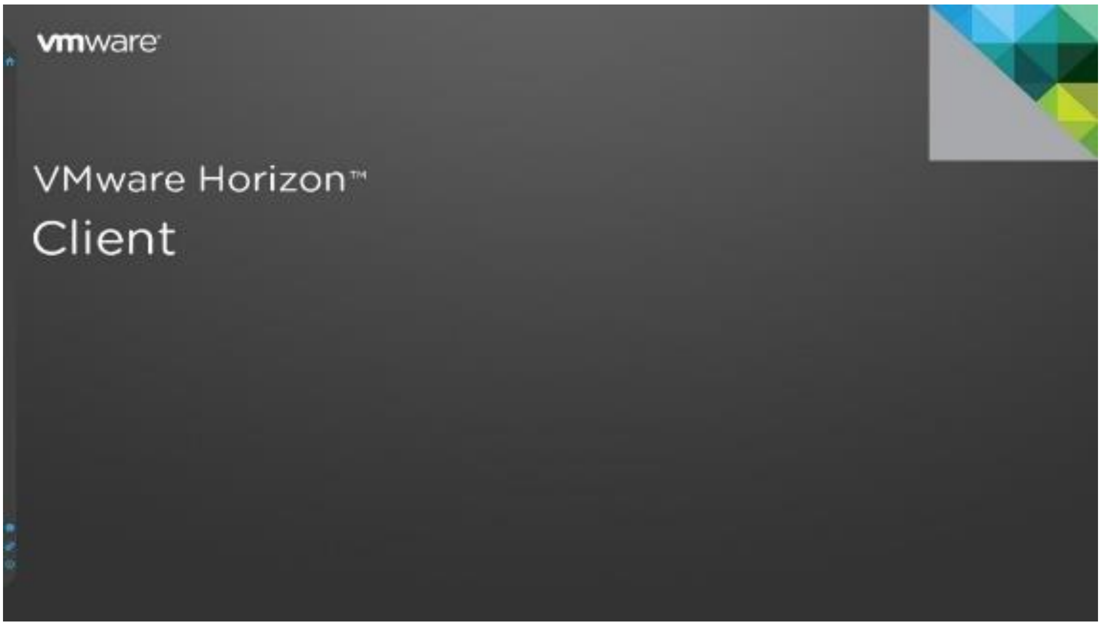
Configure a connection broker such as Citrix, VMware, Microsoft, Dell vWorkSpace, Wyse VDI or Amazon.

Your management server will overwrite your connection broker configurations.

GUI #2 Zero theme for VMware and Citrix

- Zero mode/theme for VMware and Citrix is introduced.
- INI parameter values are introduced.
    - ZeroTheme={Classic, VDI, Citrix, VMware}
    - SysMode={Classic, VDI, Citrix, VMware}
- The INI parameter works only with the **wnos.ini** file.
- Configure parameter = Citrix, system searches for **xen.ini**, and loads the Citrix zero mode (ThinOS Lite)
    - You can configure ThinOS in Citrix zero mode like using ThinOS Lite.
    - Without **xen.ini**, **wnos.ini** files will be used.
    - To switch from this mode, **wnos.ini** must be used.
- Configure parameter = VMware, system will load the VMware zero mode (new GUI)
    - You can configure ThinOS in VMware zero mode
    - VMware wallpaper is used in VMware zero mode

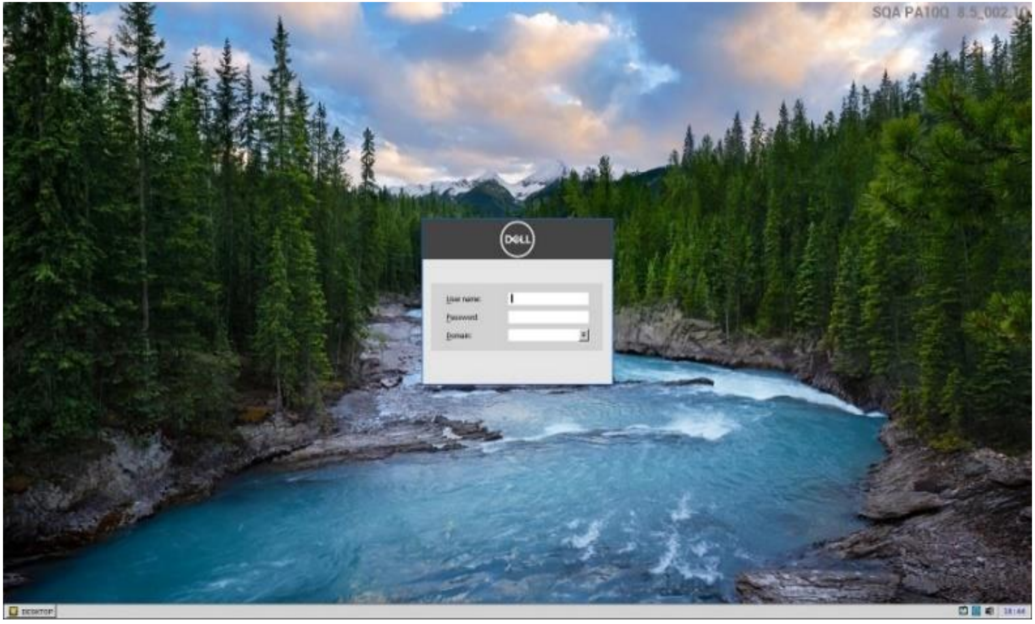


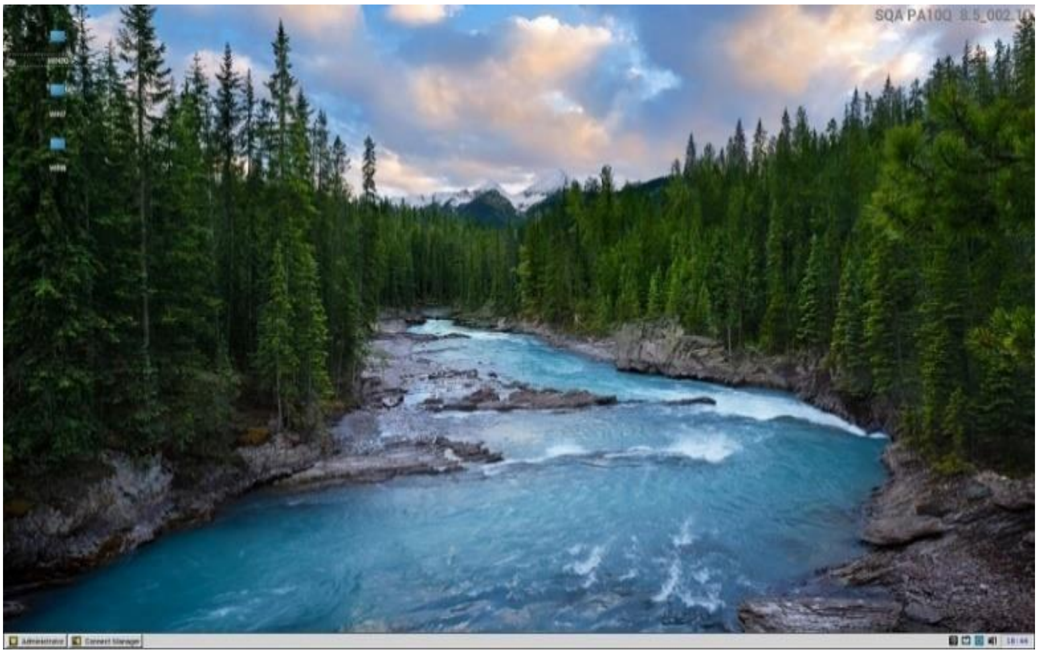


GUI #3 Added wallpaper

- This feature is not available for Wyse 3010 thin client as there is not enough memory space to store the wallpaper (930k).
- This feature is not available in zero theme (Citrix/VMware).

- Wallpaper (Standard wallpaper before and after user login)





GUI #4 System information

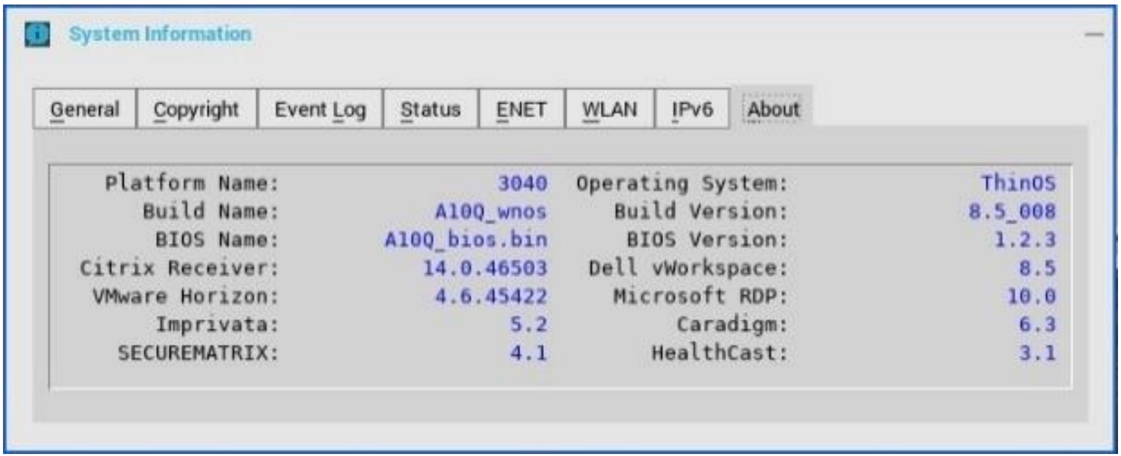
- **About** tab is added in the System Information screen with the following details:
  - ThinOS and BIOS image names (for example, **ZD10_wnos** and **ZD10_bios.bin**)
  - Citrix Broker/Receiver version (represents ICA revisions between ThinOS versions)
  - Microsoft Broker/RDP version
  - View Horizon version (this represents Horizon revisions between ThinOS versions)
  - Teradici PCoIP version (this represents PCoIP revisions between ThinOS versions)
  - Authentication (Imprivata, Secure Matrix, Caradigm, HealthCast) versions

Firmware reference details

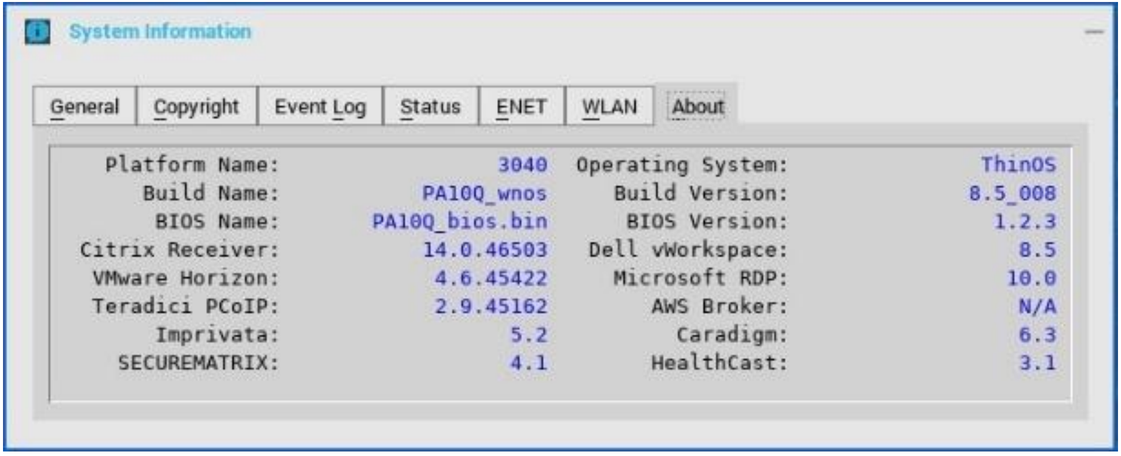
Wyse ThinOS	ThinOS	ThinOS with PCoIP
Wyse 3010 thin client	DOVE_boot	N/A
Wyse 3020 thin client	T10D_wnos	N/A
Wyse 3030LT thin client	U10_wnos	PU10_wnos
Wyse 3040 thin client	A10Q_wnos	PA10Q_wnos
Wyse 5010 thin client	ZD10_wnos	PD10_wnos
Wyse 5040 (AIO) thin client	ZD10_wnos	PD10_wnos
Wyse 5060 thin client	D10Q_wnos	PD10Q_wnos
Wyse 7010 thin client	ZD10_wnos	PD10_wnos

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, Microsoft RDP protocol version is 10.0, Imprivata version is 5.2 and so on.
- User mode –components are from the source or binary from third party and compiled or integrated into ThinOS. 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. Using this version, you can identify different revisions. For example, Citrix Receiver version is 14.0.44705, the VMware Horizon version is 4.6.45422, and so on. The components are actually matched to the installed packages. If the packages are removed, the field will be empty in the **About** tab.



```
   Platform Name:            3040  Operating System:         ThinOS
      Build Name:       A10Q_wnos      Build Version:        8.5_008
       BIOS Name:   A10Q_bios.bin       BIOS Version:          1.2.3
 Citrix Receiver:      14.0.46503   Dell vWorkspace:             8.5
  VMware Horizon:       4.6.45422      Microsoft RDP:           10.0
       Imprivata:             5.2           Caradigm:            6.3
    SECUREMATRIX:             4.1         HealthCast:            3.1
```



```
   Platform Name:            3040  Operating System:         ThinOS
      Build Name:      PA10Q_wnos      Build Version:        8.5_008
       BIOS Name:  PA10Q_bios.bin       BIOS Version:          1.2.3
 Citrix Receiver:      14.0.46503   Dell vWorkspace:             8.5
  VMware Horizon:       4.6.45422      Microsoft RDP:           10.0
  Teradici PCoIP:       2.9.45162         AWS Broker:            N/A
       Imprivata:             5.2           Caradigm:            6.3
    SECUREMATRIX:             4.1         HealthCast:            3.1
```

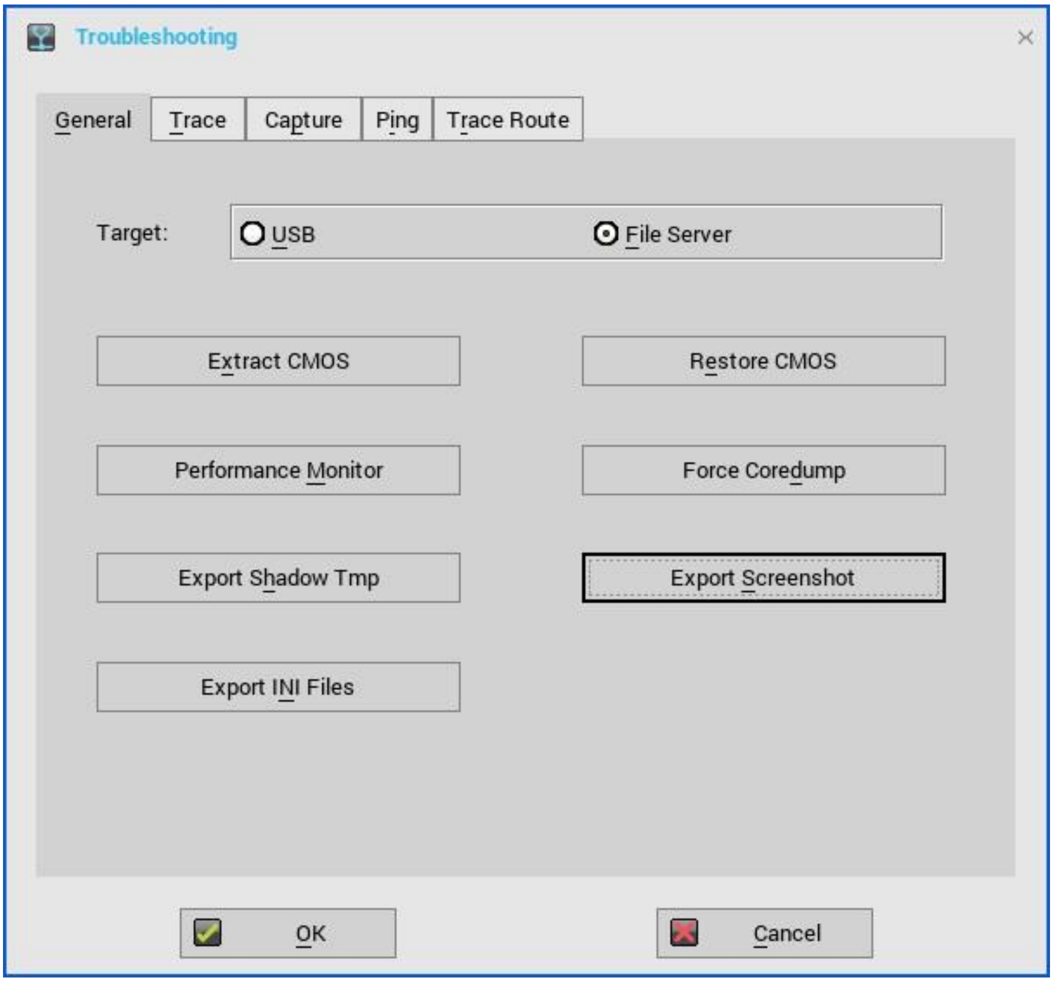
GUI #5 Trap picture export

Provides ability to save trap screenshots to the USB/File server and exports **wnos.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 **/wnos/troubleshoot/**

Working scenario

- Go to **Trouble Shooting > click Export Screen Shot**, the screen shots are exported to file server or USB key.
  - If the screen shot is copied to the clipboard, the screen shot will be exported.
  - If the screen shot is not copied to the clipboard, it will automatically copy the full screen and export.
- Go to **Trouble Shooting > click Export INI Files**, the global INI file (**wnos.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/wnos.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.

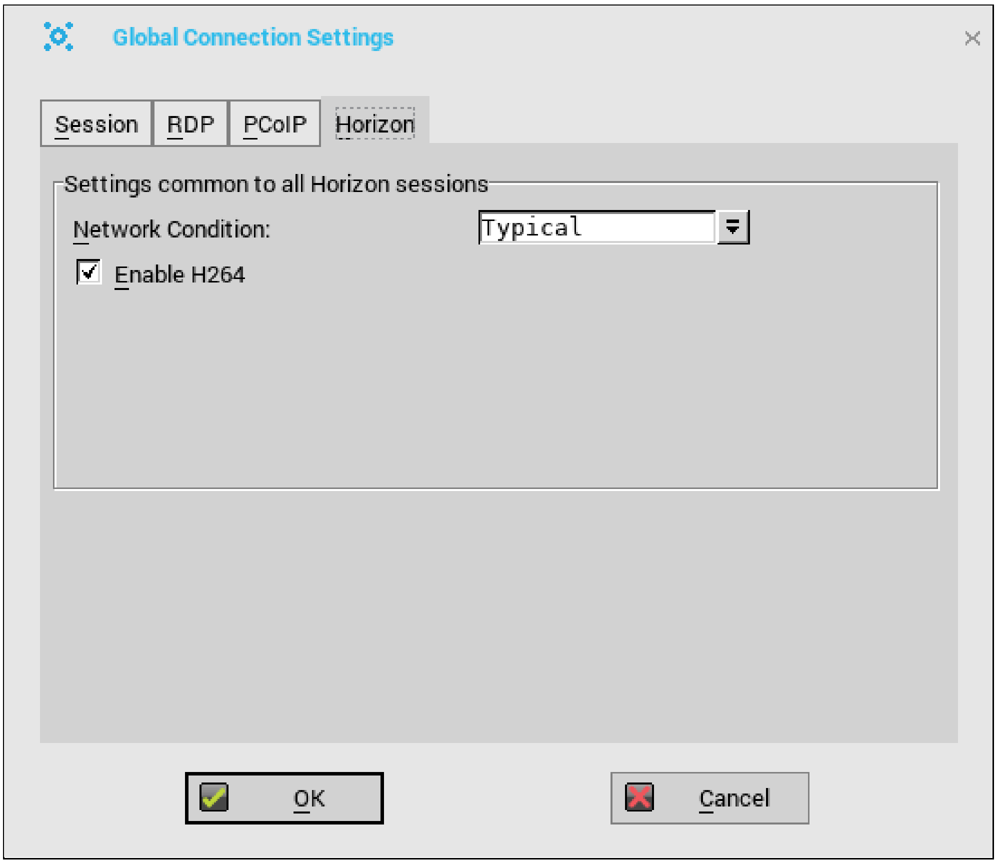

Troubleshooting

General | Trace | Capture | Ping | Trace Route

Target: ○ USB ● File Server

VMware #1 Horizon Blast Extreme H.264

- **Horizon.i386.pkg** is updated to support the new feature; see the new version and the Horizon version in the **System Information > About** tab for the revision changes.
- **Enable H264** check box is added in the **Global Connection Settings** to allow H.264 decoding for Horizon Blast Extreme (Hardware decoding).
  - This option is only available for platforms such as Wyse 3040 thin client, Wyse 5060 thin client, Wyse 3030 LT thin client.
  - The maximum resolution that is supported depends on the capability of the graphical processing unit (GPU) on the client.
- INI value **SessionConfig=Blast EnableH264=yes/no** is added for supported platforms.
  - Default is enabled in ThinOS v8.5



Settings common to all Horizon sessions

Network Condition: Typical

☑ Enable H264

Performance and Evaluation

- ThinOS implementation is based on Horizon 4.6 Linux Client
- VMware introduced performance tracker tool for evaluation and data collection
- To validate how H.264 works check the **mks** log file (**/tmp/vmware-user/vmware-mks-pid.log**) to ensure that **H264 support is enabled** is in the log file.
- Blast H.264 is not supported on Wyse 5010 thin client/Wyse 5040 thin client/Wyse 7010 thin client due to GPU driver compatibility.
- Blast H.264 is automatically disabled on Wyse 5060 thin client over 1920 x 1200 due to Hardware limitation.

Platforms	**Wyse 3040 thin client**	**Wyse 3030 LT thin client**	**Wyse 5060 thin client**	**Wyse 5010 thin client/Wyse 5040 thin client/Wyse 7010 thin client**
Blast Extreme H.264 H/W	Default is Yes			No support in 8.5 (no INI/GUI option)
Blast JPEG	INI/GUI option to switch to JPEG			Yes

VMware #2 Horizon Blast UDP/BEAT

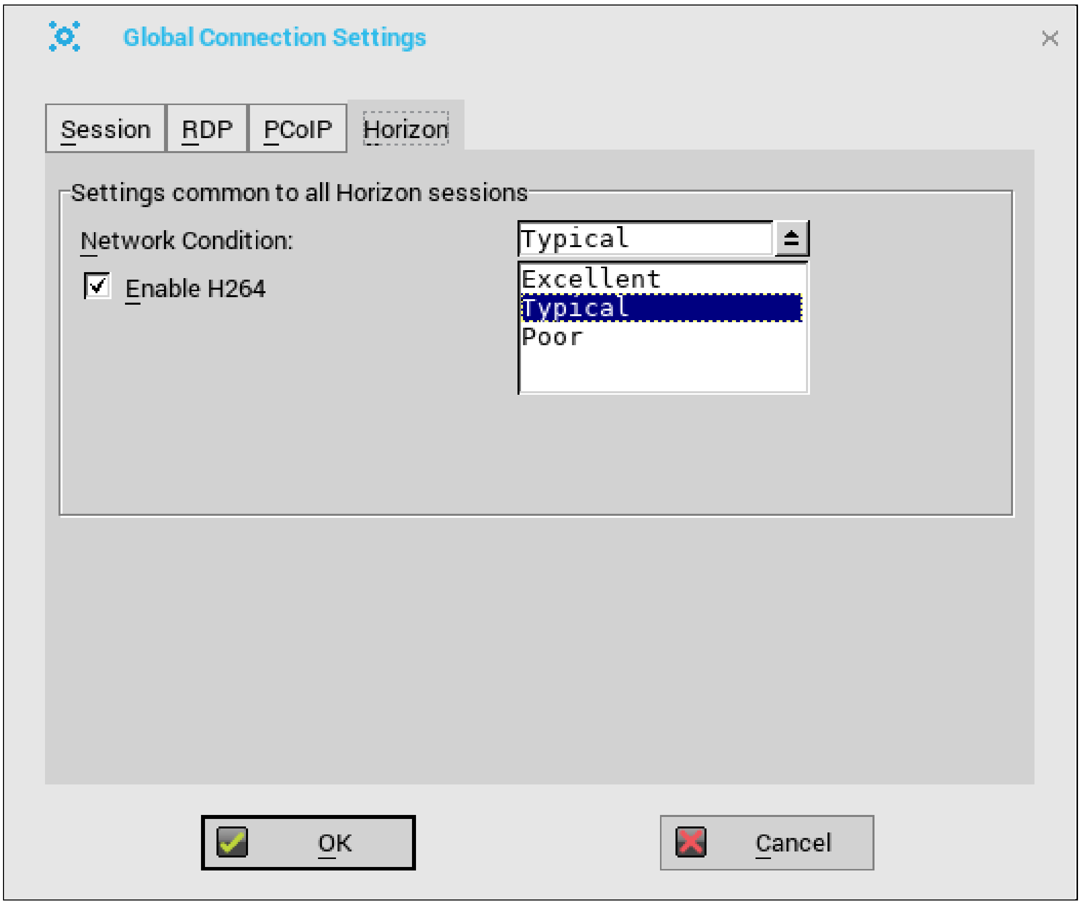
- Blast Extreme uses the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Blast Extreme as a protocol is part of BEAT (Blast Extreme Advanced Transport). Choose UDP protocol to use the bandwidth for the desired result.
- Pre-Conditions: In order to enable UDP, you need to make a few changes to the View Connection Server, the Agent host desktop as well as the Client. See, VMware guide for configuration details on the server and agent desktop.
  - The following content are from the Horizon certificate guide for reference: https://code.vmware.com/group/euc/thin-client/certs/4.6/

1. On the View Connection Server, do the following:
   a. Browse **to \Program Files\VMware\VMware View\Server\appblastgateway\absg.properties**
   b. Add the entry **enableUDP=true**. Ensure that the value is set to **true**.
   c. Restart the VMware Blast Security Gateway service.
2. To disable the Blast Secure Gateway, do the following:
   a. On your web browser, go to **View Administrator web portal**.
   b. Select View **Configuration > Servers**.
   c. Select the required Server, and click **Edit**.
   d. Deselect **Use Blast Secure Gateway for Blast Connections** to system.
3. On the Agent machine, do the following:
   a. Run **regedit** and browse to **HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Vmware Blast\Config**. Add a new string value **LogLevel** with value data set to **debug**. If **LogLevel** key already exists, change the value to **debug**.
   b. From the same location in **regedit**, add another key called **UdpEnabled** and set the data value to **1**.
   c. Run **gpedit.msc** to start the Local Group Policy Editor, under **Computer Configuration**, right click on **Administrative Templates**, and select **Add/Remove Templates**.
   d. Add the **vdm-blast.adm** entry.
   e. Click browse **Computer Configuration\Administrative Templates\Classic Administrative Templates (ADM)\VMware Blast**, ensure that H264 and UDP are enabled.
   f. Restart the Blast service.
4. Launch the Horizon Client, and connect to your View Connection Server.
5. Enable UDP from the UI.
6. Connect to a remote desktop using Blast protocol.
7. Browse to **%ProgramData%\VMware\VMware Blast\Blast-Service.log** and check the time connection was established.
8. Click **Search and confirm that socket xxx transition to state ESTABLISHED** in **Blast-Worker-SessionIdx.log. xxx** starts from 1, for example “103” message is recorded in the log file.
9. Disconnect from the remote desktop and disable UDP setting in the UI.

Working scenario in ThinOS

Select network condition in Connect Manager > Global Connection Setting > Horizon. The valid readings are:

- Excellent: this means Blast connection will use TCP
- Typical (default): this means Blast connection will use TCP
- Poor: this means Blast connection will use UDP



Settings common to all Horizon sessions

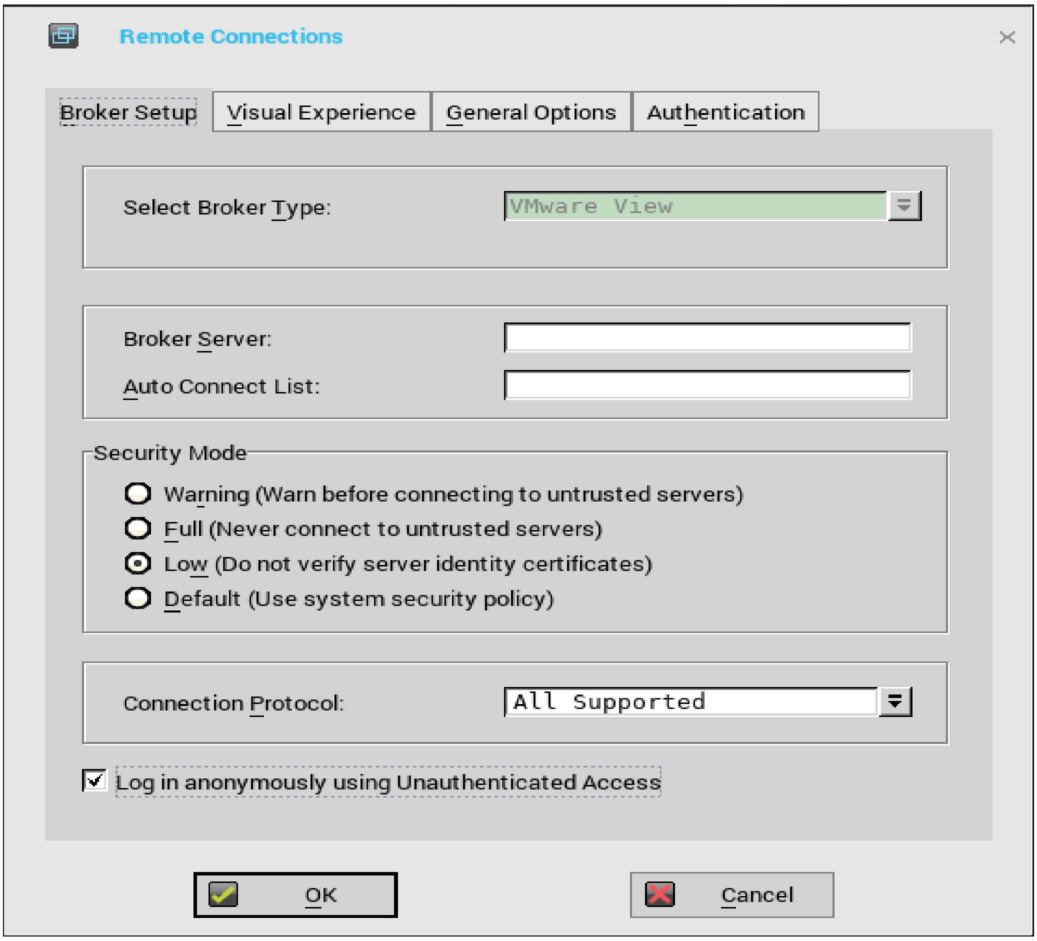
Network Condition: Typical

☑ Enable H264

VMware #3 Broker logon enhancements

Unauthenticated Users: User(s) can anonymously log into the VM remotely.

- On your AD Server, create two anonymous users. For example, **anonymous1** and **anonymous2**.
- Log in to your **View Admin** web portal.
- Go to **Users and Groups > Unauthenticated Ac**cess and add the two new anonymous users to the **View Connection Manager**.
- Under **View Configurations > select Servers > Connection Servers > select your Connection Server**, and click **Edit > Authentication tab > choose Enabled for unauthenticated access**. Do not select any users for the Default Unauthenticated User.
- Under **Application Pools > add a few applications that you have installed on this VM** and map it to **anonymous1** and **anonymous2** users.
- On ThinOS, select **Log in anonymously using Unauthenticated Access**.



Select Broker Type: VMware View

Broker Server:

Auto Connect List:

Security Mode

○ Warning (Warn before connecting to untrusted servers)

○ Full (Never connect to untrusted servers)

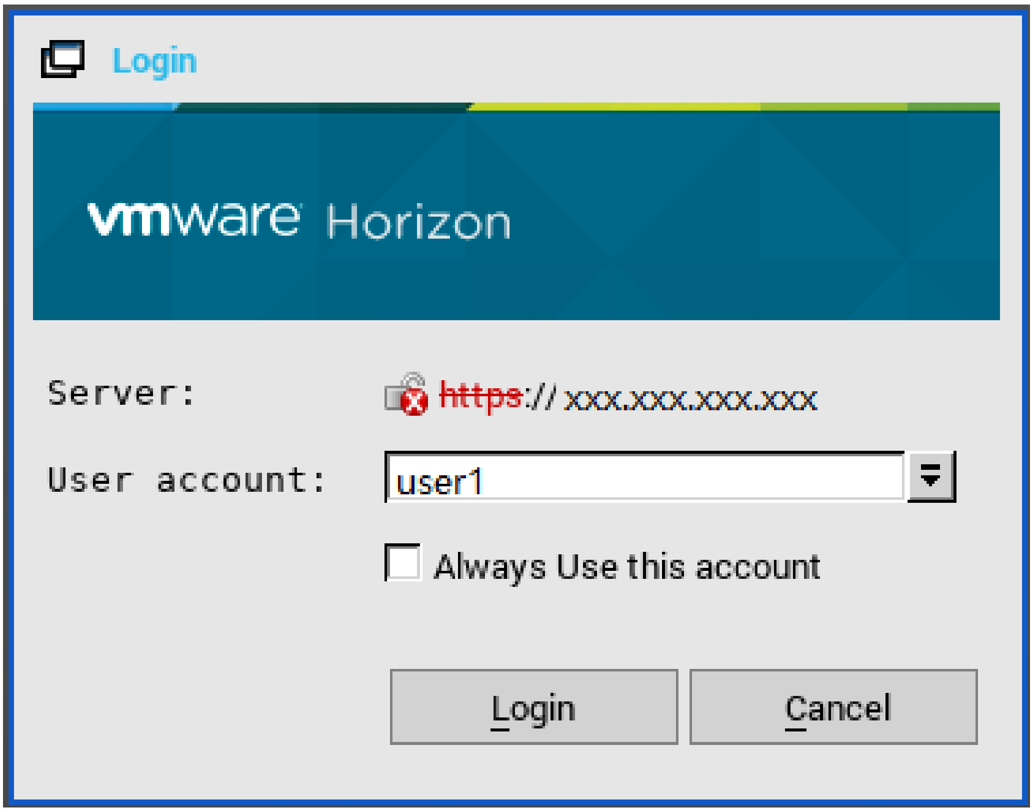
● Low (Do not verify server identity certificates)

○ Default (Use system security policy)

Connection Protocol: All Supported

☑ Log in anonymously using Unauthenticated Access

- Restart the system, and the following window is displayed:



Server: ~~https~~:// xxx.xxx.xxx.xxx

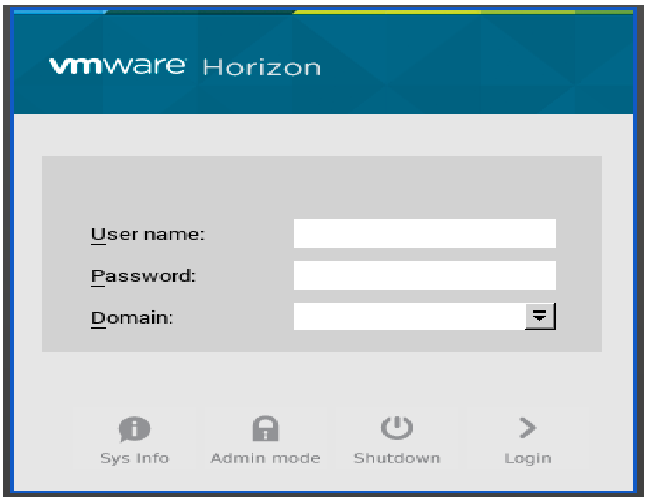
User account: user1

□ Always Use this account

- Select **Always use this account**, and you can use this account login but cannot change to other users.

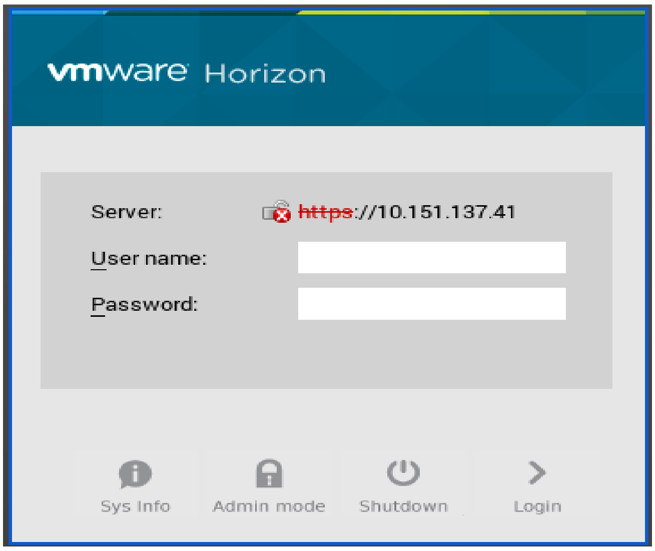
Hide Server URL: The server URL is not displayed in the Horizon View broker UI.

- Option A: Change it from View Connection Server web portal
    1. Log into your View Connection Server web portal.
    2. Under **View Configuration > Global Settings > Edit**, select the **Hide server information in client user interface** check box, clear the **hide domain list in client user interface** check box and click **OK**.
    3. Log in to VMware Horizon broker.
    4. The Server URL is not displayed when the Domain list is displayed.
- Option B: Change it using INI parameter.
    - **ConnectionBroker=vmware DisableShowServer=yes**



Hide Domain List: The domain list can be hidden in the Horizon View Broker logon UI.

1. Log into your View Connection Server web portal.
2. Under **View Configuration > Global Settings > Edit**, select the **hide domain list in client user interface** check box, clear the **Hide server information in client user interface** check box and click **OK**.
3. Restart the system.
4. The Server URL is displayed, and the Domain list is not displayed.



Server: ~~https~~://10.151.137.41

User name:

Password:

Citrix #1 Multiple audio device support

- Citrix revision in ThinOS 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.

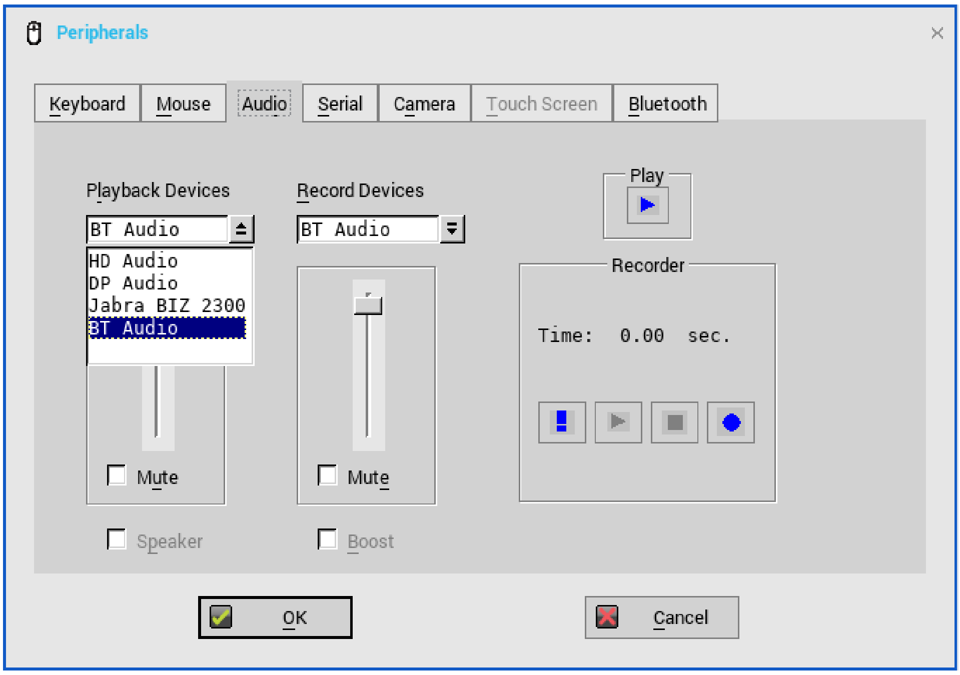
Limitation

- ThinOS 3010 and 3020 are not supported.
- For ThinOS 3030 LT, to use DP audio in session, you must set DP audio as default audio device in ThinOS Peripherals settings or the DP audio is not available in session.
- Citrix multiple audio feature does not work with HDX generic audio. The resolution for the issue will be delivered in the next ThinOS 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
  - ThinOS default audio = latest plug-in audio device.
  - Session default audio = ThinOS default audio; can be changed.
  - Upon hot plug-in/out device, advise to restart SFB/Lync client.

- UDP Audio is supported with multiple audio.
- You can switch audio device setting without hot plug-in/out.
- The multiple audio option can be shared across multiple sessions.



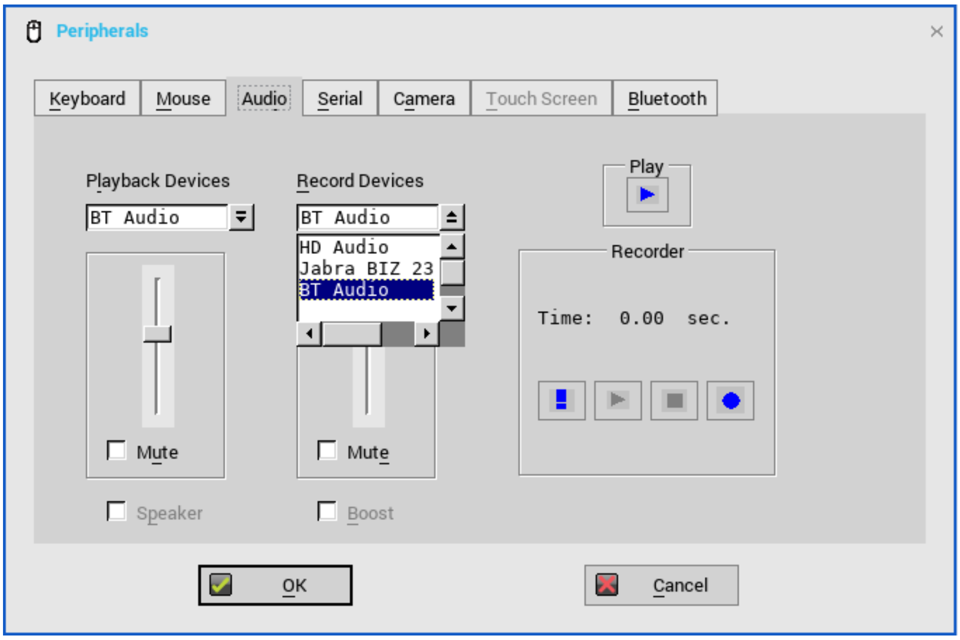
Playback Devices: BT Audio

HD Audio
DP Audio
Jabra BIZ 2300
BT Audio

Record Devices: BT Audio

Time: 0.00 sec.

□ Mute
□ Mute
□ Speaker
□ Boost



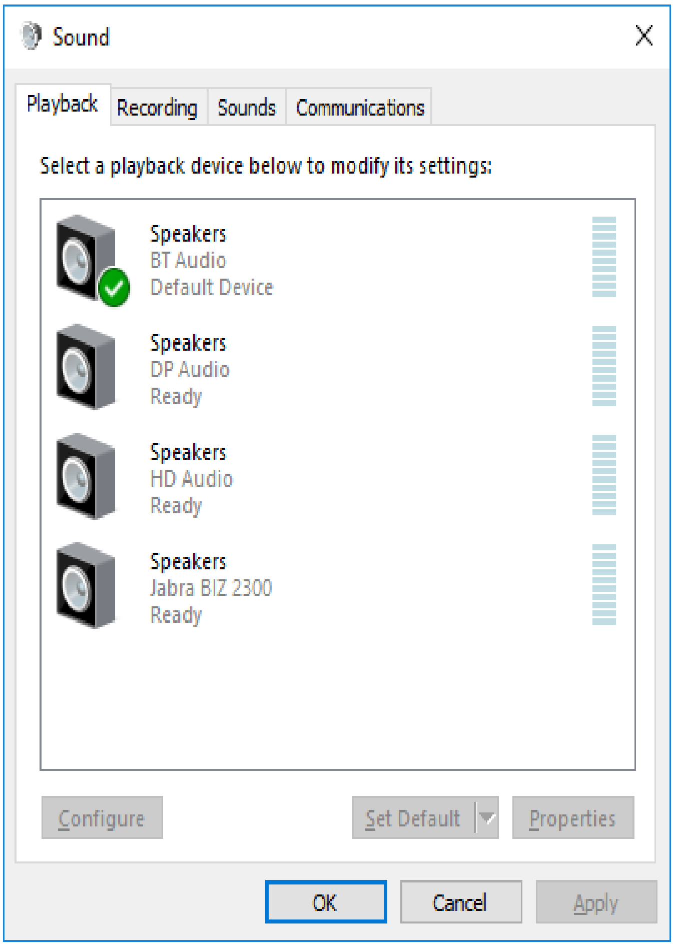
Playback Devices: BT Audio

Record Devices: BT Audio

HD Audio
Jabra BIZ 23
BT Audio

Time: 0.00 sec.

□ Mute
□ Mute
□ Speaker
□ Boost



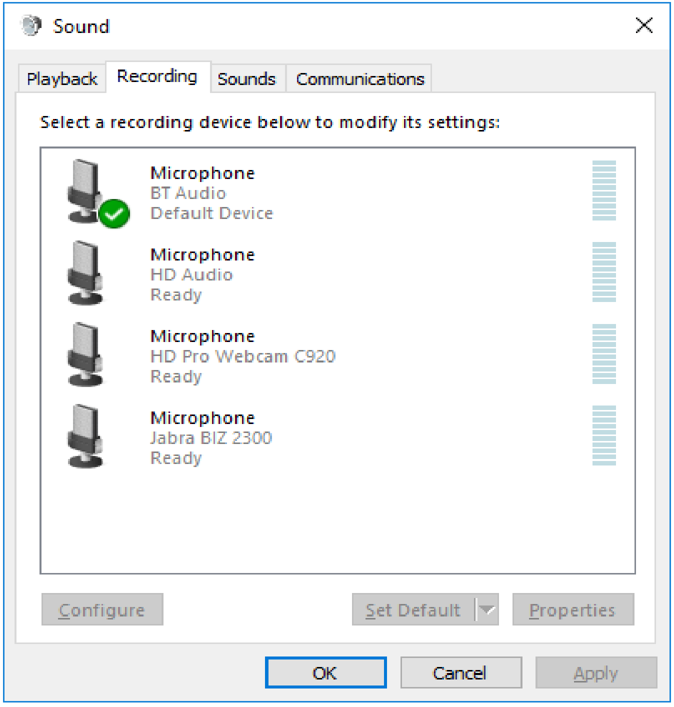
Select a playback device below to modify its settings:

Speakers
BT Audio
Default Device

Speakers
DP Audio
Ready

Speakers
HD Audio
Ready

Speakers
Jabra BIZ 2300
Ready



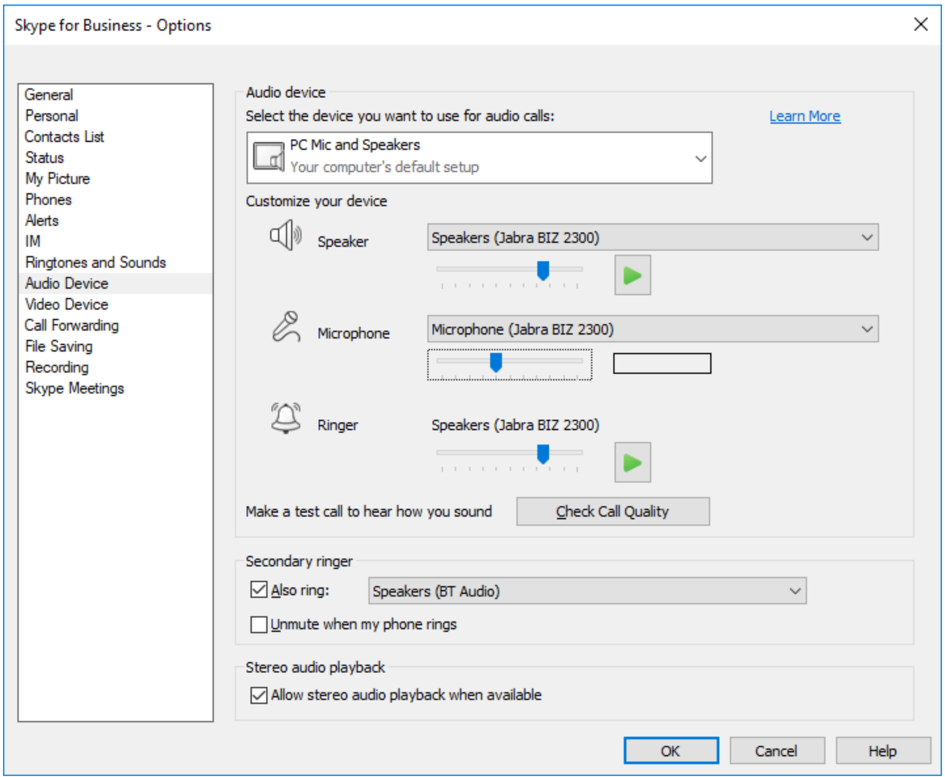
Select a recording device below to modify its settings:

Microphone
BT Audio
Default Device

Microphone
HD Audio
Ready

Microphone
HD Pro Webcam C920
Ready

Microphone
Jabra BIZ 2300
Ready



Audio device

Select the device you want to use for audio calls: PC Mic and Speakers — Your computer's default setup

Customize your device

Speaker: Speakers (Jabra BIZ 2300)

Microphone: Microphone (Jabra BIZ 2300)

Ringer: Speakers (Jabra BIZ 2300)

Make a test call to hear how you sound

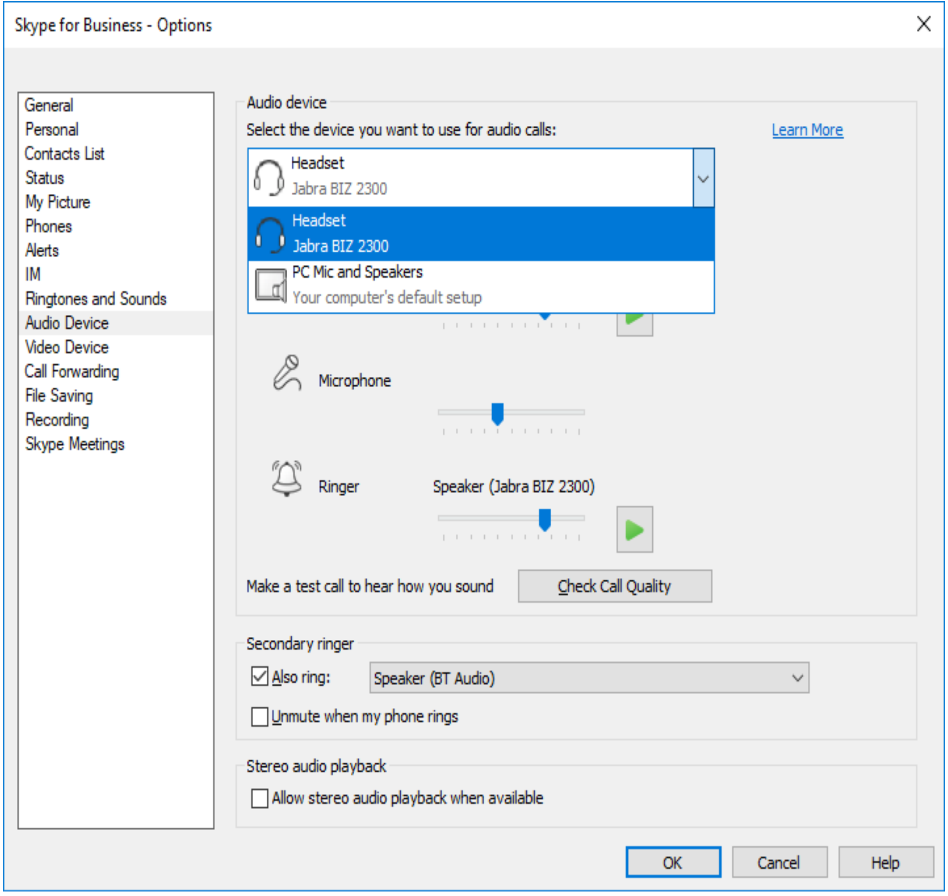
Secondary ringer

☑ Also ring: Speakers (BT Audio)

□ Unmute when my phone rings

Stereo audio playback

☑ Allow stereo audio playback when available



Audio device

Select the device you want to use for audio calls: Headset — Jabra BIZ 2300

Headset — Jabra BIZ 2300

PC Mic and Speakers — Your computer's default setup

Microphone

Ringer: Speaker (Jabra BIZ 2300)

Make a test call to hear how you sound

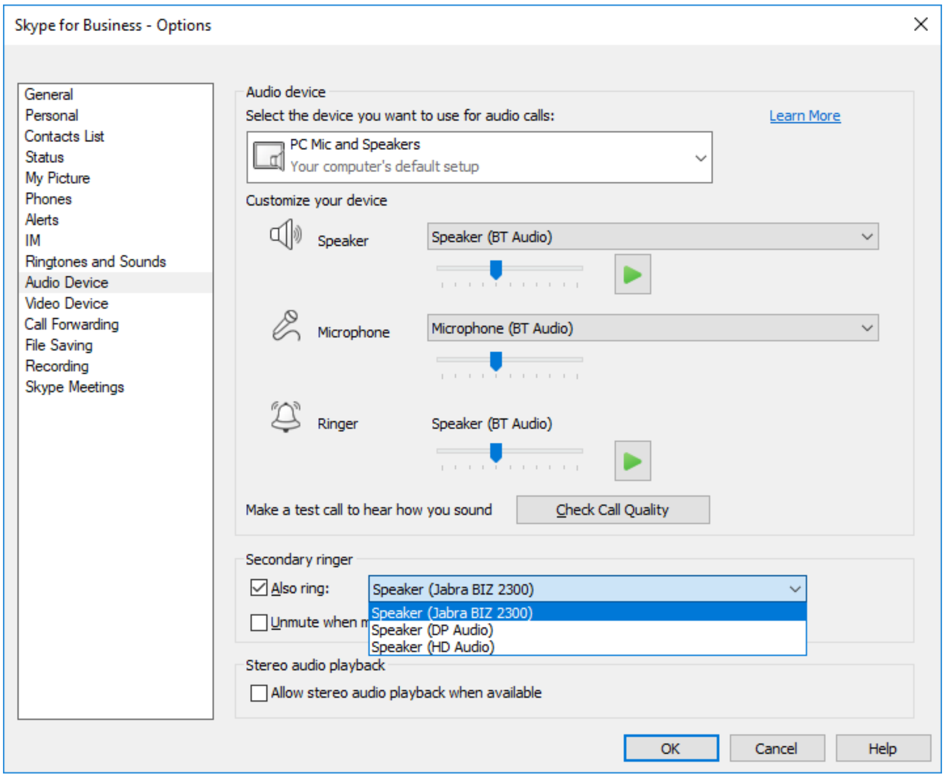
Secondary ringer

☑ Also ring: Speaker (BT Audio)

□ Unmute when my phone rings

Stereo audio playback

□ Allow stereo audio playback when available



Skype for Business - Options

Audio device

Select the device you want to use for audio calls:

PC Mic and Speakers
Your computer's default setup

Customize your device

Speaker: Speaker (BT Audio)

Microphone: Microphone (BT Audio)

Ringer: Speaker (BT Audio)

Make a test call to hear how you sound

Secondary ringer

☑ Also ring: Speaker (Jabra BIZ 2300)

□ Unmute when r

Stereo audio playback

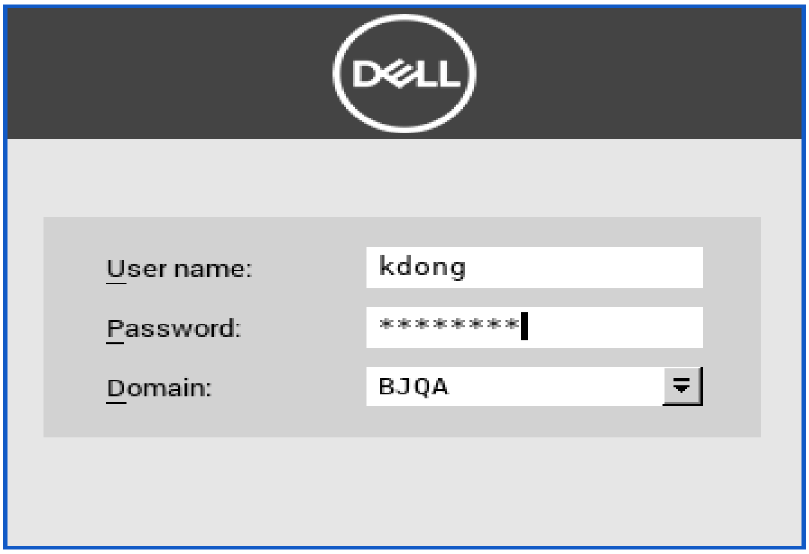
□ Allow stereo audio playback when available

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

- NetScaler 12.0 and later; SMS PASSCODE 9.0 SP1 + RADIUS
- Test message works with CensorNet App on mobile
- NetScaler RADIUS authentication policy bind with gateway server.
- You can download SMS PASSCODE 9.0 SP1 file from https://download.smspasscode.com/public/6260/SmsPasscode-900sp1.zip

Do the following for SMS passcode authentication:

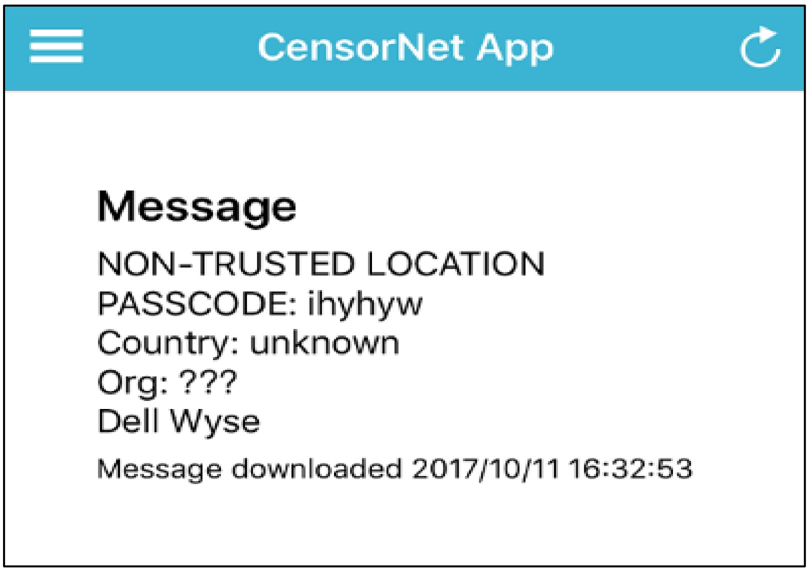
1. From ThinOS, connect the NetScaler Gateway URL.
2. Enter valid user ID and password.
3. Continue with the Passcode prompt.
4. Get the passcode from CensorNet App on mobile.
5. Enter the Passcode to complete the authentication.



User name: kdong

Password: ********

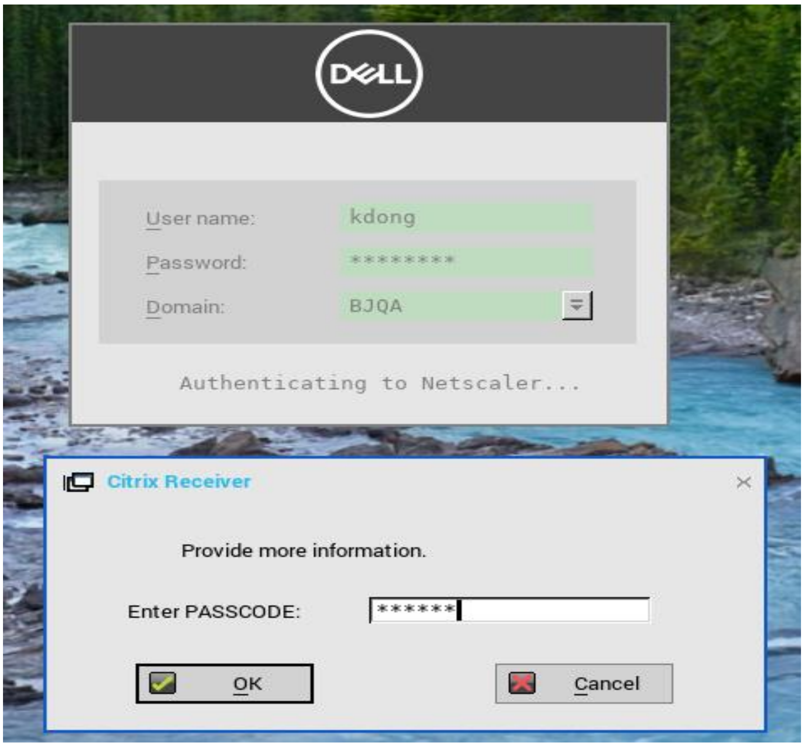
Domain: BJQA



Message

NON-TRUSTED LOCATION
PASSCODE: ihyhyw
Country: unknown
Org: ???
Dell Wyse

Message downloaded 2017/10/11 16:32:53



User name: kdong

Password: ********

Domain: BJQA

Authenticating to Netscaler...

Citrix Receiver

Provide more information.

Enter PASSCODE: ******

Citrix #3 RTME/RTOP 2.3

RTME 2.3 is included in ThinOS v8.4_110.

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 v8.5.

Microsoft RDP #1 WebSocket

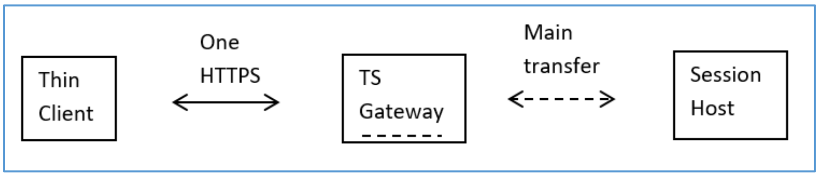
You need server 2016 with WebSocket Protocol enabled.

- In previous TS Gateway connections, the setup used is two half-duplex connections between TS Gateway server and Thin Client.
- In ThinOS 8.5, session connection setup will use duplex communication between the TS Gateway and Thin Client; Meanwhile, TSG2 and TSG3 are downward compatible. If the WebSocket connection or the TS Gateway server/Thin Client version does not support WebSocket, TSG3 or TSG2 is used.
- Compared with TSG3, if the WebSocket succeeds in the step of ‘Create OUT Channel’, then the OUT Channel and IN Channel are used the duplex communication between the TS Gateway and Thin Client, the second HTTP 1.1 connection for IN Channel will not be established.
- One HTTPS connection with WebSocket protocol can be setup in the following two steps:
  - Client setup of one HTTPS connection to TS gateway, provides handshake, authentication information and target server information.
  - Client log on to the session host server through the TS gateway connection.
  - The Network analysis file and checking the SSL Stream of the connection is upgraded to WebSocket

Server derail	TSG2	TSG3	WebSocket
Server 2008/R2	supports		
Server 2012/R2	supports	supports	
Server 2016	supports	supports	supports

TSG3 network level model
TSGU PKT
HTTPS
TCP/IP

WebSocket network level model
TSGU PKT
WebSocket Protocol
HTTPS
TCP/IP



Microsoft RDP #2 H.264 AVC444

You need RDP 10 session (Windows 10 / Server 2016) with the following policy enabled.

- **Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Remote Session Environment**:
  - Prioritize H.264/AVC 444 Graphics mode for Remote Desktop connections
  - Configure H.264/AVC hardware encoding for Remote Desktop connections

How it works

- Earlier version of ThinOS RDP H.264 uses Chroma frame 4:2:0.
- ThinOS 8.5 RDP h.264 avc444 technology uses the same decoder to process common h.264 frame and 444 mode frame. A whole 444 frame can be composed using 1 common frame and 1 extra Chroma frame.
- The feature is used to improve the image quality with artificial sharp edges and mounts of regular color boundaries, like text, so that they can be compressed using the same h.264 technology applied to other type of images.
- For RDP 8.1 session in ThinOS 8.5, it will use the original H.264 frame.
- H264-AVC444 impacts on text and images Chroma, it cannot impact on video quality.

For more information, see, https://cloudblogs.microsoft.com/enterprisemobility/2016/01/11/remote-desktop-protocol-rdp-10-avch-264-improvements-in-windows-10-and-windows-server-2016-technical-preview/

Limitation

- In ThinOS 8.5 the RDP 8.1 session uses the original H.264 frame.

- H264-AVC444 impacts the text and image Chroma, and video quality is not impacted.

DP audio

Supported information

- Monitor with DisplayPort (DP) audio is supported.
- Analog audio device in monitor DP audio interface and monitor built-in speaker are supported.
- Audio playback in ICA/RDP/Blast/PCoIP sessions, audio recording is not supported.

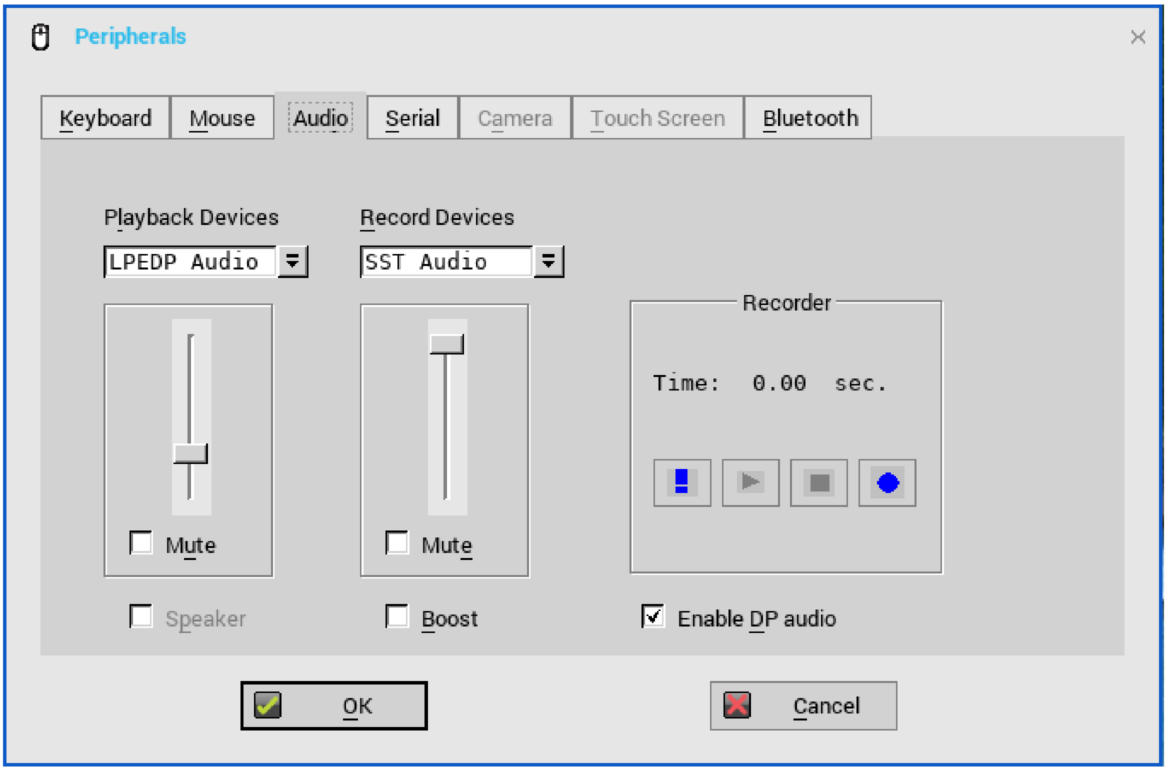
Working example

- Setup monitor with DP audio support.
- Connect ThinOS client DP port with monitor using DP cable.
- Plug in analog headset into the monitor DP audio interface.
- From ThinOS, select DP audio option from System Setup > Peripherals > Audio > Playback Devices.
- Launch an RDP or ICA (or PCoIP/Blast) session.
- Play a video and check the audio through the analog headset.

For INI configuration, see Dell Wyse ThinOS INI Reference Guide.

Disable DP audio function (For example, on Wyse 3040 thin client)

1. The DP audio by default is enabled, the 3040 thin client in certain resolution will show 10 seconds black screen after boot up (for example, 1920 x 1200, 2048 x 1152, 2048 x 1280, 2560 x 1080, 2560 x 1440). You must disable DP audio for 3040 deployment.
2. Go to thin client menu **System Setup > Peripherals > Audio- > Enable DP audio**. DP audio is enabled by default.



Playback Devices: LPEDP Audio

Record Devices: SST Audio

□ Mute

□ Mute

Time: 0.00 sec.

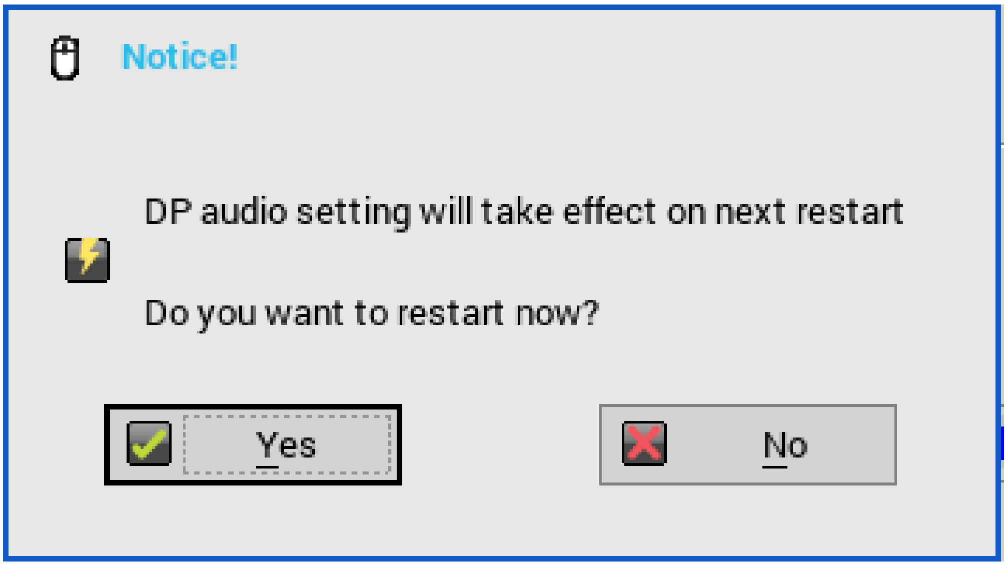
□ Speaker

□ Boost

☑ Enable DP audio

3. Do not select Enable DP audio, click Yes to restart the client.

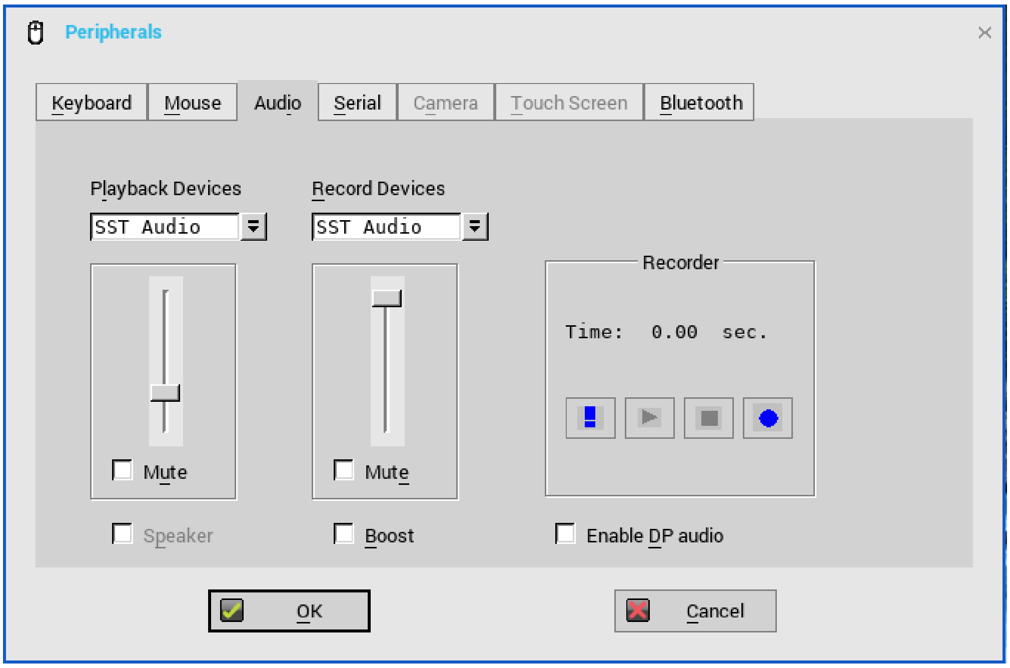
NOTE: If you select **No** in the following screen, the client will not restart and DP audio is still enabled.



DP audio setting will take effect on next restart

Do you want to restart now?

4. After reboot, go to **System Setup->Peripherals->Audio->Playback Devices**, check there is no **LPEDP Audio** option, and **Enable DP audio** is also not selected. DP Audio is now disabled.



Playback Devices: SST Audio

Record Devices: SST Audio

□ Mute

□ Mute

Time: 0.00 sec.

□ Speaker

□ Boost

□ Enable DP audio

Limitation

- Audio playback is supported. There is no support for audio recording.
- DP audio option in playback devices list on ThinOS GUI is displayed after you disable audio in BIOS setting.
- The volume cannot be changed when a video play in a blast session through DP audio

Network Settings change without need to reboot

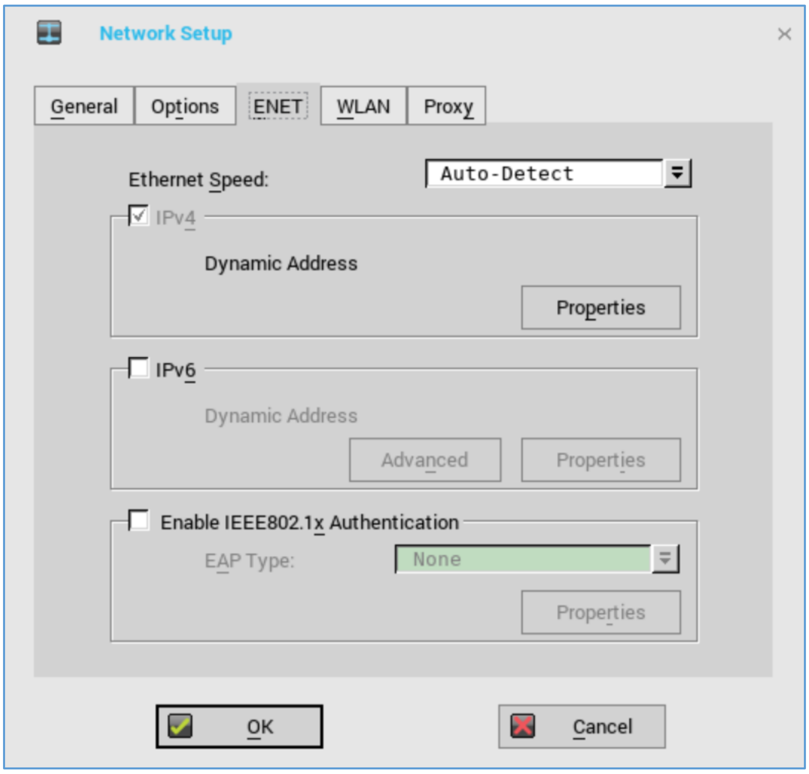
In ThinOS 8.5, any change in Network settings will not require reboot, all changes will take effect immediately.

For example,

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

Limitation

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



Ethernet Speed: Auto-Detect

☑ IPv4

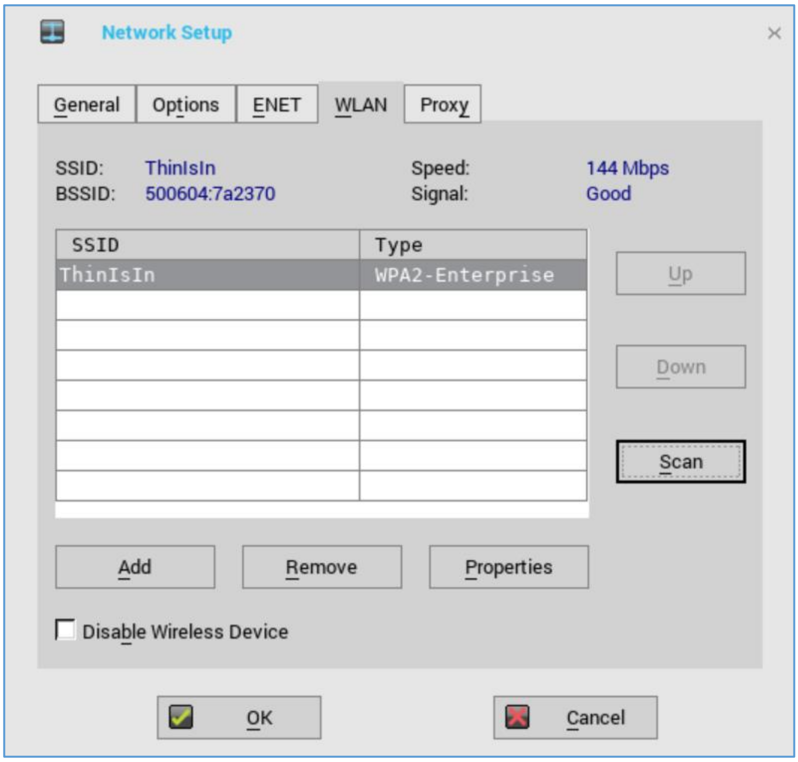
Dynamic Address

□ IPv6

Dynamic Address

□ Enable IEEE802.1x Authentication

EAP Type: None



SSID:	ThinIsIn	Speed:	144 Mbps
BSSID:	500604:7a2370	Signal:	Good

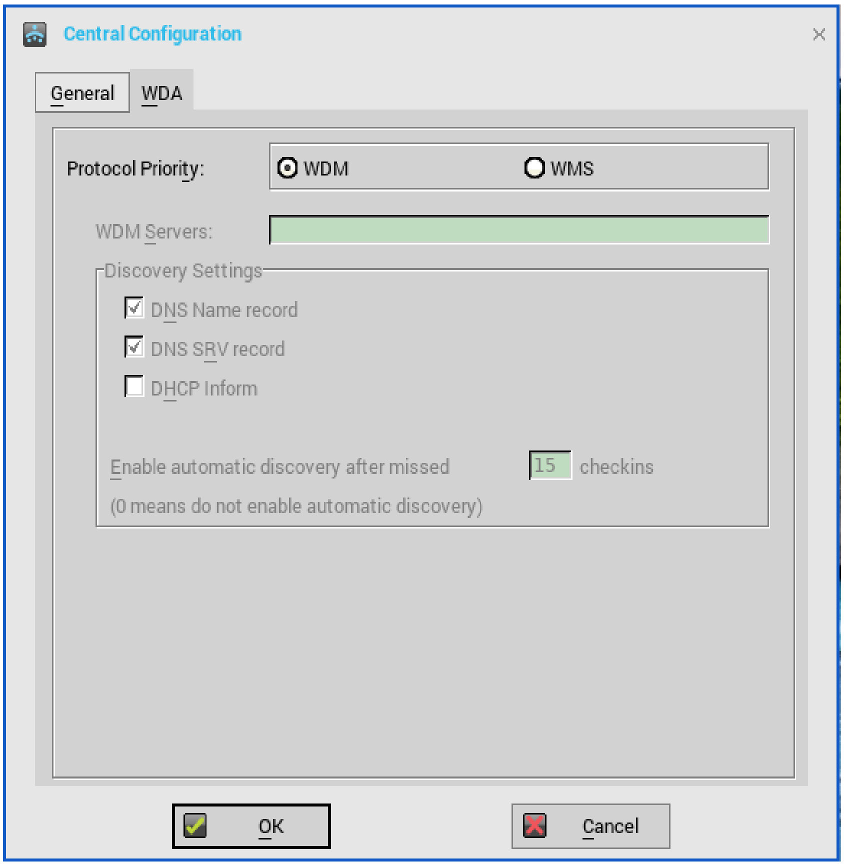
SSID	Type
ThinIsIn	WPA2-Enterprise

□ Disable Wireless Device

Wyse Device Manager/Wyse Management Suite changes

In Wyse Device Manager on ThinOS, go to **Central Configuration > WDA**.

- The default protocol is changed from WDM to WMS.
- WDM GUI can be now be disabled using one of following INI parameter.
    - WDMService=no
    - Service=wdm disable=yes
    - RapportDisable=yes



Protocol Priority: ● WDM ○ WMS

WDM Servers:

Discovery Settings

☑ DNS Name record

☑ DNS SRV record

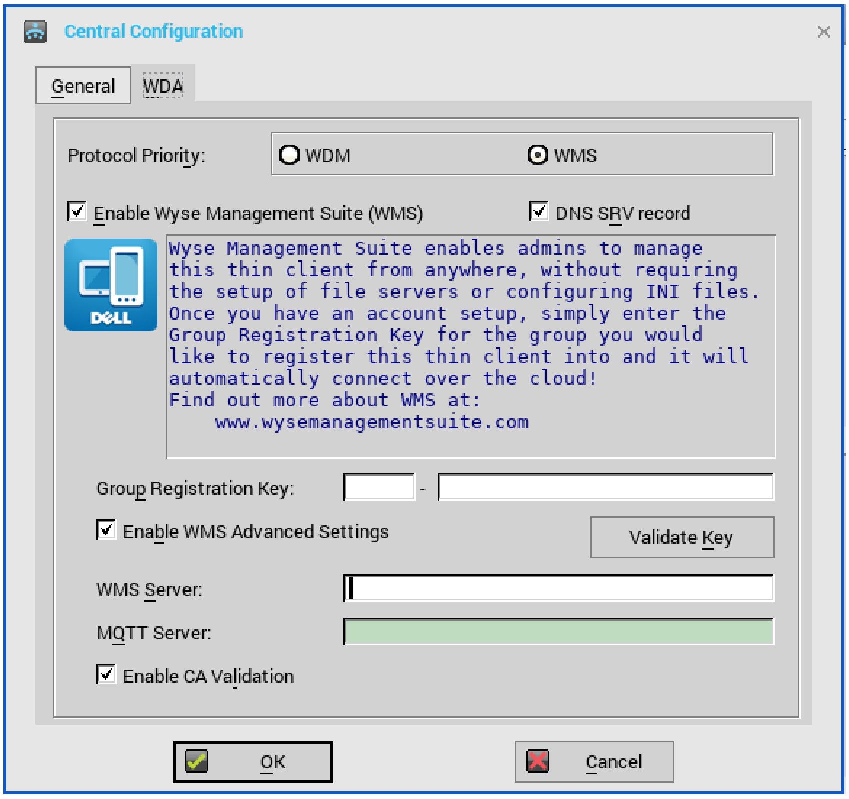
□ DHCP Inform

Enable automatic discovery after missed 15 checkins

(0 means do not enable automatic discovery)

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.



Protocol Priority: ○ WDM ● WMS

☑ Enable Wyse Management Suite (WMS) ☑ DNS SRV record

Wyse Management Suite enables admins to manage this thin client from anywhere, without requiring the setup of file servers or configuring INI files. Once you have an account setup, simply enter the Group Registration Key for the group you would like to register this thin client into and it will automatically connect over the cloud!
Find out more about WMS at:
www.wysemanagementsuite.com

Group Registration Key: -

☑ Enable WMS Advanced Settings

WMS Server:

MQTT Server:

☑ Enable CA Validation

- 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 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 v8.5 and later from Wyse Management Suite settings from the Group Policy tab.
    1. For ThinOS version earlier than 8.5, configuration is not possible from Wyse Management Suite.
    2. In ThinOS with 8.5 or later, configuration is possible from Wyse Management Suite.
    3. If you configure both "Remote Connection" and remote connection related to payload such as Broker/VDI/Connection, you need to consider the following:
        - If ThinOS version is 8.5 or later, "Remote Connection" will not be sent from Wyse Management Suite and remote connection related payload will be sent.
        - If ThinOS version is earlier than 8.5, "Remote Connection" remote connection related payload will not be 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 as follows:
    1. INI commands in INI file has the highest priority. Other payloads from UI has the lowest priority.
    2. 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:
        - Group INI overrides global group INI.

        - Device INI overrides group INI and Device INI has the highest priority.

    3. 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-8.5 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-WTOS-8.5 (INI file: Tom.ini)
            - China
                - Beijing

- Support for Wyse Management Suite Server function “Able to change CA validation for file repository”.
- Support for Wyse Management Suite Server new function “Batch Sync BIOS Admin Password Job” that only works for Wyse 3040 thin client platform using Dell BIOS.
- Support Wyse Management Suite Server function “Send heartbeat and check-in interval to the agent in ThinOS”.
    1. Whenever Wyse Management Suite agent checks-in to server, it may receive heartbeat and check-in interval if it is configured on Wyse Management Suite console, the agent should update and apply them.
    2. Whenever Wyse Management Suite agent sends heartbeat to a server, it should receive heartbeat interval and command pending flag detail.

Technical References

Wyse Management Suite registration workflow example on a Public Cloud Workflow.

- Configure ThinOS 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 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 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 devices allow secure SSL connections—`SecurityMode=Full`—only after verifying the certificates. In the current 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 release.

  The following are the workarounds to avoid the SSL connection issue:
  - Ensure that the device has a valid certificate and the correct time is selected on the device.
  - Define the server by name instead of IP address.
  - Set the value of the global security policy to high.
  - Use the following INI parameter to enforce the high security mode: `SecurityPolicy=high TLSCheckCN=Yes`
- The **base.i386** and **pcoip.i386** packages may not be available on devices:
  - Shipped with ThinOS version 8.5
  - Reimaged with a ThinOS version 8.5 Merlin image using USB imaging tool

Affected platforms	Flash size
Wyse 5010 thin client with ThinOS	4 GB or higher
Wyse 5040 thin client with ThinOS	4 GB or higher
Wyse 7010 thin client with ThinOS	4 GB or higher
Wyse 5010 thin client with PCoIP	4 GB or higher
Wyse 5040 thin client with PCoIP	4 GB or higher

  NOTE: Devices with 2 GB flash are not affected by the package issue.

  Problem statement: The following issues are observed on the affected platforms:
  - Multimedia performance issues occur because the required codecs are not available.
  - PCoIP connections are not started in Horizon View and AWS environments.
  - **Package** tab is not available in the **System Tools** menu.

  Resolution: Perform one of the following steps to resolve the issue on the affected devices:
  - Use the 4 GB Merlin image to flash the devices with 4 GB flash configuration. Use the 8 GB Merlin image to flash the devices with 8 GB flash and higher configurations.
  - Install the ThinOS 8.5 web image to reload the missing package files. You can install the ThinOS web image by using either a file server, Wyse Device Manager (WDM), or Wyse Management Suite. If the ThinOS web image is stored on a file server or management server, and if the automatic image update option is enabled using the INI parameter `Autoload=1 LoadPkg=1` is enabled, then the device automatically installs the **base.i386** or **pcoip.i386** packages during system reboot.
- 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.
- Display: With DP audio by default enabled, the Wyse 3040 thin client in certain resolution will display 10 seconds' black screen after boot up (for example. 1920 x 1200, 2048 x 1152, 2048 x 1280, 2560 x 1080, 2560 x 1440).
- Blast connection: if there any is launch problem check the remote desktop status as well as network status; reboot unit few times and the desktop connects successfully.

- Boot up unit without monitor or with monitor power-off.
  - Wyse 5010 thin client/Wyse 5040 thin client/Wyse 7010 thin client/Wyse 3030 LT thin client: 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.
  - Wyse 3040 thin client /Wyse 5060 thin client: the client waits until the monitor is attached or power on.
- From ThinOS version 8.5, 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>
<tr><th>INI Parameter</th><th>Description</th></tr>
<tr><td>SysMode={classic, vdi, VMware*, Citrix*}</td><td>SysMode= specifies the system mode which has different GUI.
Classic mode has full taskbar, desktop and connection manager. This is recommended for terminal server environment, and for backward compatibility with ThinOS 6.x.
VDI mode (Badger GUI) has new launchpad-style GUI designed for VDI. You can access through an overlay interface. Recommended for VDI or any full-screen only connections.
* VMware mode is like VDI mode but allows VMware horizon broker. Login window and wallpaper is specified for horizon.
Citrix mode will make client turn to ThonOS Lite. Xen.ini file is considered during next reboot.
* VMware mode and Citrix mode can only be used in wnos.ini.
SysMode has another alias name "ZeroTheme", you can also use ZeroTheme=xxx in wnos.ini.</td></tr>
<tr><td>ScreenSaver=value
[Type={0,1,2,3,4}]
[VideoLink=httplink]*
[VideoSpan=no]*
[Unit=hour]*</td><td>
<table>
<tr><td>Value</td><td>Delay Before Starting</td></tr>
<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>
</table>
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.
*The optional parameter Unit=hour converts screen saver timer value from minutes to hours to set a longer time.
The optional parameter `Type` specifies which type of screen saver to use
<table>
<tr><td>Value</td><td>Type of Screen Saver</td></tr>
<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>
<tr><td>3</td><td>Showing Pictures</td></tr>
<tr><td>4</td><td>Playing Video*</td></tr>
</table>
</td></tr>
</table>

INI Parameter	Description
	*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.

Device=cmos
[AutoPowerDate={yes,no}]*
[AutoPowerTime={hh:mm:ss}*
[AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]*
	[[AutoPowerDate={yes,no}]*
	
	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] in the INI settings refers to the BIOS system time and not the ThinOS system time.
	
	The time
	
	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}]
	
	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

Device=cmos [CurrentPassword=password]* [CurrentPasswordEnc=password encrypted]* [NewPassword=password]* [NewPasswordEnc=password encrypted]*	*[CurrentPassword= password NewPassword = password] This option is used to change device's BIOS password (CurrentPassword is not required if device's BIOS password is not existed). The Max count of password string is 19 bytes. [CurrentPasswordEnc=password encrypted] This option is used to provide encrypted current password. [NewPasswordEnc=password encrypted] This option is used to provide encrypted new password. Note: Password encrypted will be higher priority. For example, If CurrentPassword and CurrentPasswordEnc both configured, CurrentPasswordEnc will overwrite the CurrentPassword.
Device=DellCmos [PXEBootSupport={yes, no}]]*	[PXEBootSupport={yes, no}] If yes is specified, devices allows OS to boot from PXE. If no is specified, OS cannot boot device from PXE.
Device=DellCmos [USBBootSupport={yes, no}]*	[USBBootSupport={yes, no}] If yes is specified, devices allows OS to boot from USB port. If no is specified, OS cannot boot device from USB port. Note: USB keyboard and mouse always work regardless of specified or not.

Device=DellCmos
Action={extract, restore}*
	For extract action, CMOS content is saved to file $PF_cmos.$VER ($PF – name of Dell BIOS platform, including X10 and A10Q)

INI Parameter	Description
	($VER – version of BIOS, like 1.2.2. With a WTOS log: "CMOS: extract to $PF_cmos.$VER" For restore action, CMOS content is updated from file $PF_cmos.$VER With a syslog, CMOS: restore from $PF_cmos.$VER The file is strongly checked and protected from corruption. 1. The content is wrapped in a file header, including a field of magic number, checksum, timestamp, length and platform name. 2. The content is first checksum and then AES encrypted during save operation. 3. On restore operation, If the CMOS timestamp (stored in nvram) matches the timestamp on the file, the cmos content will not be written every time to avoid wearing out the cmos chip. For usage of this feature, there should be a special INI user name like "cmos". The associated ini/cmos.ini should include one line as "Device=DellCmos Action=extract" (Pleaset note: "Device=DellCmos Action=extract" is not suggested to be written in global INI file, like wnos.ini, and it will take no effect if it has been written in global INI file). And “CurrentPassword” is must be required if device's BIOS password is existed regardless extract or restore action. For example, Device=DellCmos CurrentPassword= xxxxx Action=restore After the administrator configured the CMOS on a template unit, the administrator should sign on to "cmos" account on WTOS to get the CMOS content saved to the cmos file on writable File Server wnos directory. Then, the wnos.ini should be configured with "Device=DellCmos action=restore", so all target units will get updated with the same CMOS setting as template unit after reboot. Once the restore action is finished, both the "Device=DellCmos Action=extract" and "Device=DellCmos action=restore" should be removed from the related INI files. The usage of other settings is self-explanatory. The only condition to use the setting is the BIOS GUI has such settings.
PRIVILEGE=[None, Low, High] [FastDHCP={yes,no}]*	FastDHCP will identify gateway first, if it's same as the network before disconnection and previous DHCP information isn't expired, use previous DHCP information and won't start a new DHCP process. Default is yes.
VPN=openconnect [Username-enc=encrypted_username_string]* [Password-enc=encrypted_password_string]*	It configures the OpenConnect VPN session. It can allow up to 4 connections. • The option "Username-enc" specifies AES encrypted Login Username • The option "Password-enc" specifies AES encrypted Login Password
Folder=[folder]*	Folder for grouping the connections. Display the folder on ThinOS desktop only if classic mode and set "signon=yes icongroupstyle=folder". The folder can include sub folder, for example, connect=rdp host=10.151.122.71 icon=default folder=rdp\test1
$DHCP(extra_dhcp_option)	Extra DHCP options which are for win CE unit, including 169, 140, 141, 166, 167 For example, set a string "test169" for option tag 169 in DHCP server, set TerminalName=$DHCP(169) in wnos.ini Check terminal name in GUI, the terminal name will be "test169". The 166 and 167 is default for WMS/CCM MQTT Server and WMS/CCM CA Validation in ThinOS.

INI Parameter	Description
	So need to remap the options from GUI or INI if want to use $DHCP(166) and/or $DHCP(167).
SessionConfig=ICA [ClientName=_client_name_]*	"ClientName" can specify the client name for ICA session, the default is terminal name. It can use system variable, for example, SessionConfig=ICA ClientName=$mac NOTE: The mac address includes a special character ':'. This may cause the following issue. TIR94401: Etoken Java(aladdin) and Etoken CardOS SmartCard fail to logon XenDesktop 7.15 desktop.
PnliteServer=List of {IP address, DNS names or URLs} [SFIconSortMode={0, 1, 2, 3}]*	A list of host names or IP addresses with optional TCP port number or URLs of PN-Lite servers. Default = Empty. Each entry with optional port is specified as Name-or-IP:port, where :port is optional, if no 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 “,” or “;” to separate servers that belong to different farms. SFIconSortMode will sort storefront dekstop icon. 0, default value, sort by the position value from server side. 1, sort in alphabetic. 2, sort in alphabetic with desktop first. 3, sort in alphabetic with application first. Others, same with 0.

Device=audio
[DPaudio=yes,no]*
[local_button=yes, no]*
	DPaudio=[yes, no]
	Default option is DPaudio=yes. DP audio may impact display on A10Q with some screen resolution (1920x1200, 2048x1152, 2048x1280, 2560x1080, 2560x1440(U2718Q, UP3216Q) listed but not limited, user needs to disable DP audio via ini or GUI. This setting only works for terminals have DP audio support (A10Q, D10Q, and U10).
	
	local_button=[yes, no]
	Default option is local_button=yes, if local_button=no, it will make mute/volume up/volume down button be disabled in ThinOS local, but it works during session

SessionConfig=Blast [EnableH264={yes,no}]*	Control the Blast H264 feature on the supported platforms. Default = yes. The value yes means enable H264; the value no means disable H264. This works on Blast H.264 supported platforms.

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

Fixed issues

SL No.	Description
1	Citrix Receiver logo display quality improvements 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 8.5 firmware

Tested environments matrix

The following are the tested server versions for the release; this is not an environment support matrix; the supported versions are not limited to the tested versions.

Wyse Management Suite	1.1
Wyse Device Manager	5.7.2
Imprivata OneSign	5.2.0.15
Caradigm	6.3.1
NetScaler	9.3/10.0/10.1/10.5/11.0/11.1/12.0
StoreFront	3.6/3.11/3.12
Web Interface	5.4
SecureMatrix	4.1.0

	Win7	Win8.1	Win10	Linux	W2K8R2	W2K12R2	W2K16	APPs
VM Horizon 7.3	√	√	√	√	√	√	√	√
XD 5.6	√							
XA 6.5					√			√
XD/XA 7.6	√	√			√	√		√
XD/XA 7.15	√	√	√		√	√	√	√
Tera PCM for AWS 1.03	√ *							
RDS 2012R2/2016	√	√	√			√	√	√

*AWS Workspace VM OS “Windows 7 style” is actually based on 2008R2 RDSH

XD/XA	OS	RTME	Lync client	Lync server	SFB Server
7.6	Win8.1	1.8	Lync 2013	Lync 2013	
	W2K12R2	2.3	SFB2015		SFB2015
7.15	Win7	2.3	SFB2016		SFB2015
	Win10	2.3	SFB2016		SFB2015

	Win8.1	2.3	SFB2016		SFB2015
	W2K16	2.3	SFB2016		SFB2015

Tested peripherals matrix

The following are the tested devices for the release, and the supported devices are not limited to the tested devices only.

ECO system validation matrix

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	Dell USB 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

SQA peripherals validation matrix

Peripheral Name	**Type**	**Device Comments**	**Brand/Model**
Dell E2416Hb (1920x1080)	Monitor		Dell E
Dell E2715Hf (1920x1080)	Monitor		Dell E
Dell UP3216Qt(3480X2160)	Monitor		Dell UP
Dell P2415Q(3480X2160)	Monitor		Dell P
Dell P2714Hc (1920x1080)	Monitor		Dell P

Peripheral Name	Type	Device Comments	Brand/Model
Dell P2715Q(3840x2160)	Monitor		Dell P
Dell P2815Qf (3840x2160)	Monitor		Dell P
Dell U2713Hb (2560x1440)	Monitor		Dell U
Dell U2713HM (2560x1440)	Monitor		Dell U
Dell U2713HMt (2560x1440)	Monitor		Dell U
Dell U2718Qb (3840x2160)	Monitor		Dell U
Dell U2718Q (3480X2160)	Monitor		Dell U
Dell U2913 WM (2560x1080)	Monitor		Dell U
Dell U3014t (2560x1600)	Monitor		Dell U
Dell S2817Q(3840x2160)	Monitor		Dell S
Dell UZ2315H (1920x1080)	Monitor		Dell UZ
Dell 3008WFP (2560x1600)	Monitor		Dell
Dell P2418HT(1920x1080)	Touch Screen		Dell P
Dell B1163 Mono Multifunction Printer	Printer	Printer USB redirection only	Dell
Dell B1165nfw Mono Multifunction Printer	Printer	Printer USB redirection only	Dell
Dell B1260dn Laser Printer	Printer		Dell
Dell B1265dnf Multifunction Laser Printer	Printer		Dell
Dell B2360d Laser Printer	Printer		Dell
Dell B2360dn Laser Printer	Printer		Dell
Dell B2375dnf Mono Laser Multifunction Printer	Printer		Dell
HP LaserJet P2055d	Printer		HP
HP LaserJet P2035	Printer		HP
HP LaserJet 1022n	Printer		HP
HP Color LaserJet CM1312MFP	Printer		HP
EPSON PLQ-20K	Printer		EPSON
Dell KM636 Wireless Keyboard and Mouse	Keyboard/mouse		Dell
DELL wireless Keyboard/mouse KM632	Keyboard/mouse		Dell
DELL wireless Keyboard/mouse KM714	Keyboard/mouse		Dell
Dell Keyboard KB212-B	Keyboard/mouse		Dell
Dell Keyboard KB216p	Keyboard/mouse		Dell
Dell Mouse MS111-P	Keyboard/mouse		Dell
Dell Mouse MS116-P	Keyboard/mouse		Dell

Peripheral Name	**Type**	**Device Comments**	**Brand/Model**
Dell Keyboard SK-3205 (Smartcard reader)	Keyboard/mouse		Dell
Dell Optical Wireless Mouse – WM123	Keyboard/mouse		Dell
Dell Wireless Mouse – WM324	Keyboard/mouse		Dell
Dell Wireless Bluetooth Travel Mouse – WM524	Keyboard/mouse	Bluetooth	Dell
Logitech K480 Keyboard, Bluetooth	Keyboard/mouse	Bluetooth	Logitech
Logitech K400 Plus	Keyboard/mouse		Logitech
Logitech M557 mouse, Bluetooth	Keyboard/mouse	Bluetooth	Logitech
Microsoft Arc Touch Mouse 1428	Keyboard/mouse		Microsoft
Microsoft ARC touch mouse 1592, Bluetooth	Keyboard/mouse	Bluetooth	Microsoft
Microsoft Designer Bluetooth Keyboard/Mouse	Keyboard/mouse	Bluetooth	Microsoft
Rapoo E6100, BlueTooth	Keyboard/mouse	Bluetooth	Rapoo
Cherry RS 6700 USB (Smartcard reader)	Keyboard/mouse		Cherry
SpaceNavigator 3D Space Mouse	Keyboard/mouse		3DCONNEXION
Jabra PRO 935 MS	USB Headset		Jabra
Jabra PRO 9450	USB Headset		Jabra
Jabra PRO 9470, Bluetooth	USB Headset	Bluetooth N/A for ThinOS	Jabra
Jabra Speak 510 MS, Bluetooth	USB Headset	Bluetooth	Jabra
Jabra Evolve 75	USB Headset		Jabra
Jabra Evolve 40 MS Mono	USB Headset		Jabra
Jabra UC SUPREME MS /LINK 360, Bluetooth	USB Headset		Jabra
Jabra UC Voice 550 MS Duo	USB Headset		Jabra
Jabra GN2000	USB Headset		Jabra
Plantronics BLACKWIRE C420	USB Headset		Plantronics
Plantronics BLACKWIRE C520	USB Headset		Plantronics
Plantronics SAVI W740/Savi W745	USB Headset	Bluetooth N/A for ThinOS	Plantronics
Plantronics SAVI W740 3IN1 Convertible, UC, DECT 6.0 NA, Bluetooth	USB Headset		Plantronics
Plantronics SAVI List 400 series	USB Headset		Plantronics
Plantronics Voyager Legend UC B235 NA, Bluetooth	USB Headset	Bluetooth	Plantronics

Peripheral Name	Type	Device Comments	Brand/Model
Plantronics Calisto P240 D1K3 USB handset	USB Headset		Plantronics
Plantronics Calisto 620-M, Bluetooth	USB Headset	Bluetooth	Plantronics
Plantronics DA60	USB Headset		Plantronics
Plantronics P420	USB Headset		Plantronics
Plantronics USB DSP DA40(B)	USB Headset		Plantronics
SENNHEISER USB SC230	USB Headset		SENNHEISER
SENNHEISER SP 20 ML Speakerphone for Lync and mobile devices	USB Headset		SENNHEISER
SENNHEISER SC 660 Binaural CC&O HS, ED	USB Headset		SENNHEISER
SENNHEISER SC 260 USB MS II	USB Headset		SENNHEISER
SENNHEISER SP 10 ML Speakerphone for Lync	USB Headset		SENNHEISER
SENNHEISER D 10 USB ML-US Wireless DECT Headset	USB Headset		SENNHEISER
SENNHEISER DW Pro2 ML	USB Headset		SENNHEISER
SENNHEISER SC 75 USB MS	USB Headset		SENNHEISER
SENNHEISER MB Pro 2 UC ML	USB Headset	Bluetooth	SENNHEISER
POLYCOM Deskphone CX300	USB Headset		POLYCOM
LFH3610/00 SPEECHMIKE PREMIUM	SPEECHMIKE PREMIUM		PHILIPS
LFH3200/00 SPEECHMIKE PREMIUM	SPEECHMIKE PREMIUM		PHILIPS
LFH3210/00 SPEECHMIKE PREMIUM	SPEECHMIKE PREMIUM		PHILIPS
Dell USB Soundbar AC511	Audio soundbar		Dell
Logitech C525 HD Webcam	USB Webcam		Logitech
Logitech C920 HD Pro Webcam	USB Webcam		Logitech
Logitech C930e HD Webcam	USB Webcam		Logitech
Logitech BCC950 ConferenceCam	USB Webcam		Logitech
Logitech USB Webcam 9000	USB Webcam		Logitech
Logitech ConferenceCam CC3000e	USB Webcam		Logitech
Microsoft LifeCam 3.0 Cinema	USB Webcam		Microsoft
Microsoft LifeCam HD-3000	USB Webcam		Microsoft
SanDisk USB 3.0 16GB	Data storage		SanDisk

Peripheral Name	Type	Device Comments	Brand/Model
SanDisk Extreme USB 3.0 16G	Data storage		SanDisk
Kingston DataTraveler 100 G3	Data storage		Kingston
Kingston DataTraveler G3 16GB	Data storage		Kingston
Kingston DataTraveler G3 8GB	Data storage		Kingston
Kingston DataTraveler Elite 3.0 16G	Data storage		Kingston
Kingston DTM30 32GB	Data storage		Kingston
ADATA S107/16GB	Data storage		ADATA
ADATA S102/16GB	Data storage		ADATA
ADATA UV150 USB 3.0 16GB	Data storage		ADATA
BENQ DVD Drive	USB DVD RW		BENQ
SAMSUNG PorTable DVD Writer SE-208	USB DVD RW		SAMSUNG
Dell SW316	USB DVD RW		Dell
HTC one-XL	Mobile Phone		HTC
iPhone 7	Mobile Phone		Apple
Samsung Galaxy 7	Mobile Phone		Samsung
DP-DVI Convertor	Converter Display		N/A
DP-VGA Convertor	Converter Display		N/A
Dell DP-VGA convertor	Converter Display		Dell
Dell DP-DVI KKMYD convertor	Converter Display		Dell
Cisco GLC-T 30-1410-03 B2 V03	Converter Network		Cisco
TRANSITION SGFEB 1040-120	Converter Network		TRANSITION
Prolific USB-to-Serial converter U232-P9V2	Converter USB		Prolific
USB-to-Serial converter	Converter USB		N/A
Dell Keyboard M/N KB813	Smartcard Reader		Dell
Dell Keyboard SK-3205	Smartcard Reader		Dell
Cherry keyboard RS 6600	Smartcard Reader		Cherry
Cherry keyboard RS 6700	Smartcard Reader		Cherry
Cherry keyboard KC 1000 SC	Smartcard Reader		Cherry
Gemalto IDBridge CT710	Smartcard Reader		Gemalto
OMNIKEY OK CardMan3121	Smartcard Reader		OMNIKEY
HID OMNIKEY 3021	Smartcard Reader		OMNIKEY
HID OMNIKEY 5125	Smartcard Reader		OMNIKEY
HID OMNIKEY 5421	Smartcard Reader	Support smartcard only	OMNIKEY

Peripheral Name	Type	Device Comments	Brand/Model
HID OMNIKEY 5325 CL	Smartcard Reader		OMNIKEY
SmartOS powered SCR335	Smartcard Reader		SmartOS
Actividentity USB reader 2.0	Smartcard Reader		Actividentity
RDR-80581AKU	Proximity Card Reader		
RDR-80582AKU	Proximity Card Reader		
RDR-6082AKU	Proximity Card Reader		
OMNIKEY 5025 CL	Proximity Card Reader		OMNIKEY
OMNIKEY 5326 DFR	Proximity Card Reader		OMNIKEY
OMNIKEY 5427 CK	Proximity Card Reader		OMNIKEY
OMNIKEY 5125	Proximity/Smartcard Reader		OMNIKEY
OMNIKEY 5325 CL	Proximity/Smartcard Reader		OMNIKEY
Finger Print Keyboard ET710	Fingerprint Reader		
Oberthur ID One 128 v5.5	Smartcard CAC	SHA256 included	
G&D FIPS 201 SCE 3.2	Smartcard CAC	SHA256 included	
Gemalto TOPDLGX4 144	Smartcard	SHA256 included	
SafeNet SC650	Smartcard SiPR		

Smart card information

Smart Card info from ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 6.2	ActivClient Cryptographic Service Provider	Oberthur CosmopoIC 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 CosmopoIC 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