# **Dell Wyse ThinOS**

Version 8.6 Administrator's Guide



#### Notes, cautions, and warnings

i NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

MARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2018 — 2020 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

Chapter 1: Introduction	
About this guide	-
Technical support	
What is new in ThinOS 8.6_412	
What is new in ThinOS 8.6_303	8
What is new in ThinOS 8.6_206	8
What is new in ThinOS 8.6_027	(
What is new in ThinOS 8.6_024	(
What is new in ThinOS 8.6_019	10
What is new in ThinOS 8.6_013	10
Chapter 2: Before working on ThinOS	12
Firmware upgrade and package deployment	12
Firmware upgrade using HTTPS	
Firmware upgrade using Wyse Management Suite	14
Firmware installation using Dell Wyse USB Imaging Tool	14
BIOS upgrade	14
Upgrading BIOS on Wyse 5060 thin client and Wyse 3030 LT thin client	15
Upgrading BIOS on Wyse 3040 thin client	16
Upgrading BIOS on Wyse 5070 thin client	16
Upgrade BIOS on the Wyse 5470 Thin Client	17
Upgrade BIOS on the Wyse 5470 All-in-One Thin Client	17
System configuration and deployment	18
How to set up fingerprint using Wyse Device Manager	18
Automating updates and settings using central configuration	19
How to set up automatic updates and configurations	19
Chapter 3: Getting started	23
End User License Agreement	23
Configuring ThinOS using the First Boot Wizard	23
Connecting to a remote server	28
Connecting a remote server manually	29
Using your desktop	
Configuring thin client settings and connection settings	30
Connecting to a printer	30
Connecting to a monitor	30
Locking the thin client	30
Signing off and shutting down	30
Battery information	
Sleep mode	
Enable sleep manually	
Enable automatic sleep	
Additional getting started details	
Zero desktop features	33

Zero interactive desktop guidelines	33
Zero toolbar	34
List of connections	34
Using Zero theme	35
Classic desktop features	35
Classic interactive desktop guidelines	35
Using the Shortcut menu	36
Using the desktop menu	36
Using the Connection Manager	36
Login dialog box features	37
Word wrap feature	
Accessing system information	
ENERGY STAR compliance	
IPv6 certification	
hapter 4: Global Connection settingshapter 5: Configuring connectivity	
Configuring the network settings	
Configuring the general settings	
Configuring the DHCP options settings	
Configuring the ENET settings	
• •	
Configuring the WLAN settings	
Configuring the proxy settings	
Configuring the broker setup	
Configuring the visual settings	
Configuring the general options	
Configuring the authentication settings	
Configuring the central configurations	
Configuring the general central configurations	
Configuring the Wyse Device Agent settings	
Configuring the VPN Manager	80
hapter 6: Configuring the connection brokers	
Configuring Citrix	
Configuring the Citrix broker connection	
Citrix Receiver feature matrix	
Citrix HDX RealTime Multimedia Engine or RealTime Optimization Pack	
Cisco Jabber Softphone for VDI	
Using Citrix ADC	
Citrix Cloud services	
Citrix icon refresh	
Using multiple audio in Citrix session	
Configuring ICA connections	
Support for multi-monitors in Citrix session	102
ICA Self Service Password Reset	103
QUMU or ICA Multimedia URL Redirection	109
HTML5 Video Redirection	109

ICA SuperCodec	110
Anonymous logon	112
Configuring the Citrix UPD printer	112
Flash Redirection	116
Configuring VMware	
Configuring the VMware broker connection	118
VMware Horizon Client feature matrix	119
Using VMware Horizon View broker and desktop	124
Enable username hint for smart card login	125
Supporting VMware Real Time Audio-Video	126
VMware Blast	128
VMware Horizon Virtualization Pack for Skype for Business	130
Using multi-monitors in PCoIP session	132
Using Multi-monitors in VMware Blast session	133
Blast Virtual Printing	
Enable hardware cursor in Blast session	136
Enable relative mouse feature	
USB device splitting in Blast session	137
Supporting Teradici SDK	
Configuring PCoIP connections using Teradici Remote Workstatic	
Customize PCoIP login window and icons	
Configuring Microsoft Remote Desktop	
Configuring the Microsoft Remote Desktop broker connection	
Configuring RDP connections	
Features of RDP protocol	
Configuring Dell vWorkspace	
Configuring the Dell vWorkspace broker connection	
Configuring Amazon Web Services or WorkSpaces	
Configuring the Amazon WorkSpaces broker connection	
Configuring Teradici Cloud Access	
Configuring the Teradici Cloud Access broker connection	153
Chapter 7: Configuring local settings	155
Local Settings Menu	155
Configuring the system preferences	155
Configuring the display settings	157
Configuring the peripherals settings	168
Configuring the printer settings	178
Reset features	
Resetting to factory defaults using G-Key reset	
Resetting to factory defaults using shutdown reset	
Resetting display settings using V-Key reset	182
Chapter 8: TCX Suite	183
Chapter 9: Trusted Platform Module version 2.0	184
Chapter 10: Performing diagnostics	195
System tools	
- , · · · · · · · · · · · · · · ·	

Simplified Certificate Enrollment Protocol	188
About Default Certificates	189
Using the troubleshooting options	196
Chapter 11: BIOS management on ThinOS	204
Accessing BIOS settings	205
CMOS central management and extracting CMOS settings to the file server for distribution	205
CMOS local management and extracting CMOS settings to a USB key for distribution	206
Dell Standard BIOS management	207
hapter 12: Security	209
Firmware signature	209
Transport Layer Security	210
Smart cards and smart card readers	210
Rutoken smart card reader	210
Chapter 13: Troubleshooting	211
	212
ppendix A: Examples of common printing configurations	2 <b>12</b> 212
Appendix A: Examples of common printing configurations  Printing to local USB or parallel printers	<b>212</b> 212 212
Appendix A: Examples of common printing configurations  Printing to local USB or parallel printers	212 212 212
ppendix A: Examples of common printing configurations  Printing to local USB or parallel printers  Using the Printer Setup dialog box for local USB or parallel printers  Printing to non-Windows network printers	212 212 213 213
ppendix A: Examples of common printing configurations  Printing to local USB or parallel printers	212 212 212 213 213
Printing to local USB or parallel printers  Using the Printer Setup dialog box for local USB or parallel printers  Printing to non-Windows network printers  Using the Printer Setup dialog box for non-Windows network printers  Using INI parameters for non-Windows network printers	212 212 213 213 214
Printing to local USB or parallel printers	212 212 213 213 214 214
ppendix A: Examples of common printing configurations  Printing to local USB or parallel printers  Using the Printer Setup dialog box for local USB or parallel printers  Printing to non-Windows network printers  Using the Printer Setup dialog box for non-Windows network printers  Using INI parameters for non-Windows network printers  Printing to Windows network printers  Using the Printer Setup dialog box for Windows network printers	212 212 213 213 214 214 214
ppendix A: Examples of common printing configurations.  Printing to local USB or parallel printers.  Using the Printer Setup dialog box for local USB or parallel printers.  Printing to non-Windows network printers.  Using the Printer Setup dialog box for non-Windows network printers.  Using INI parameters for non-Windows network printers.  Printing to Windows network printers.  Using the Printer Setup dialog box for Windows network printers.  Using INI parameters for Windows network printers.	212 212 213 214 214 214 215
Appendix A: Examples of common printing configurations.  Printing to local USB or parallel printers	212 212 213 213 214 214 215 215
ppendix A: Examples of common printing configurations.  Printing to local USB or parallel printers  Using the Printer Setup dialog box for local USB or parallel printers  Printing to non-Windows network printers  Using the Printer Setup dialog box for non-Windows network printers  Using INI parameters for non-Windows network printers  Printing to Windows network printers  Using the Printer Setup dialog box for Windows network printers  Using INI parameters for Windows network printers  Using your thin client as a print server  Using the Printer Setup dialog box for configuring LPD services.	212212213214214214215215
Printing to local USB or parallel printers  Using the Printer Setup dialog box for local USB or parallel printers  Using the Printer Setup dialog box for non-Windows network printers  Using the Printer Setup dialog box for non-Windows network printers  Using INI parameters for non-Windows network printers  Printing to Windows network printers  Using the Printer Setup dialog box for Windows network printers  Using INI parameters for Windows network printers  Using your thin client as a print server  Using the Printer Setup dialog box for configuring LPD services  Using INI parameters for configuring LPD services	212212213214214214215215216
Printing to local USB or parallel printers	212212213214214214215216216

# Introduction

Thin clients running Dell Wyse ThinOS firmware are designed solely for optimal thin client security and performance. These efficient purpose-built thin clients are virus and malware resistant and offer ultrafast access to applications, files and network resources within Citrix, Microsoft, VMware and Dell vWorkspace environments, and other leading infrastructures. ThinOS based thin clients are self-managed, go from power-on to fully productive in seconds, and with no published API, locally accessible file system or browser, require no local McAfee Anti-Virus software or firewall to protect against viruses or malware.

# **About this guide**

This guide is intended for administrators of thin clients running Wyse ThinOS. It provides information and detailed system configurations to help you design and manage a ThinOS environment.

#### **Supported Products**

This guide is intended for the following Dell Wyse ThinOS products:

- · Wyse 3020 Thin Client with ThinOS (T10D)
- Wyse 3030 LT Thin Client with ThinOS
- Wyse 3030 LT Thin Client with PCoIP
- Wyse 3040 Thin Client with ThinOS
- Wyse 3040 Thin Client with PColP
- Wyse 5010 Thin Client with ThinOS (D10D)
- Wyse 5010 Thin Client with PCoIP (D10DP)
- Wyse 5040 AIO Thin Client with ThinOS (5212)
- Wyse 5040 AIO Thin Client with PCoIP (5213)
- · Wyse 5060 Thin Client with ThinOS
- · Wyse 5060 Thin Client with PCoIP
- Wyse 5070 Thin Client with ThinOS
- · Wyse 5070 Thin Client with PCoIP
- Wyse 5070 extended Thin Client with ThinOS
- Wyse 5070 extended Thin Client with PCoIP
- Wyse 7010 thin client with ThinOS (Z10D)
- Wyse 5470 Thin Client with ThinOS
- Wyse 5470 Thin Client with PCoIP
- Wyse 5470 All-in-One Thin Client with ThinOS
- Wyse 5470 All-in-One Thin Client with PCoIP

#### Finding the information you need in this guide

You can use either the Search window or Find toolbar to locate a word, series of words, or partial word in an active PDF document. For detailed information on using these features, refer to the Help in your PDF reader.

# **Technical support**

To access technical resources self-service portal, knowledge base, software downloads, registration, warranty extensions/ RMAs, reference manuals, contact information and so on, visit www.dell.com/wyse/support.

# What is new in ThinOS 8.6\_412

The following are the new features or updates to the existing features in this release:

#### Zero desktop update

New network icons are added to the taskbar on the Zero desktop. For more information, see Zero interactive desktop guidelines.

#### · RDP update

Supports Remote Desktop Session (RDS) 2019 from this version onwards. For more information, see *Dell Wyse ThinOS 8.6 Release Notes* at www.dell.com/support.

#### · INI updates

- Added a new INI parameter for Teradici cloud access. For more information, see Dell Wyse ThinOS 8.6 INI Guide at www.dell.com/support.
- Added new INI parameters for Ethernet and Wireless MAC addresses. For more information, see *Dell Wyse ThinOS 8.6 INI Guide* at www.dell.com/support.
- o Supports secure RDP connections using INI parameters. For more information, see Secure RDP.

#### ThinOS enhancements

- o Updated the Cipher Suits. For more information, see Dell Wyse ThinOS 8.6 Release Notes at www.dell.com/support.
- Added the End User License Agreement to ThinOS. For more information, see End User License Agreement.
- o Improved the wake time from automatic sleep mode. For more information, see Enable automatic sleep.
- Supports 5K resolution on selected monitors. For more information, see VMware Horizon Client feature matrix.
- o Supports Bloomberg keyboard. For more information, see VMware Horizon Client feature matrix.
- Supports Cryptovision smart card driver. For more information, see Smart cards and smart card readers.
- o Supports sleep mode on Wyse 5070 Thin Client. For more information, see Sleep mode.
- Updated the mouse cursor speed levels. For more information, see Configuring the mouse settings.
- o Added a warning message to Central Configuration. For more information see Configuring the general central configurations.

# What is new in ThinOS 8.6\_303

The following are the new features or updates to the existing features in this release:

- · Added the Network icon to taskbar on ThinOS classic desktop. See, Classic interactive desktop guidelines.
- Ability to view the Wyse Management Suite group token using the Show Key option. See, Configuring the Wyse Device Agent settings.
- · Ability to change the registration code for Amazon WorkSpaces. See, Configuring the Amazon WorkSpaces broker connection.
- Ability to define the Wyse Management Suite Proxy information using DHCP options or DNS SRV records. See, Configuring the proxy settings.
- Supports RC4\_HMAC\_MD5 for RDP connections. See, Configuring Microsoft Remote Desktop.
- · Supports TicTok smart cards. See, Smart cards and smart card readers.
- Ability to limit core dumps by clearing Non-Volatile Random Access Memory (NVRAM). See, the Dell Wyse ThinOS 8.6 INI guide at www.dell.com.support.

NOTE: Support for Wyse 3010 Thin Client has been depreciated since it is end of software support. There are no updates for Flash Redirection (FR) and TCX packages from this release onwards.

# What is new in ThinOS 8.6\_206

The following are the new features or updates to the existing features in this release:

#### · Updates to ThinOS packages

Updated the JVDI package to version 12.6.19091611.

#### · Citrix Receiver updates

Updated the Citrix Receiver on ThinOS to version 14.0.19071816.

#### · Amazon WorkSpaces updates

- o Supports Multi-factor authentication (MFA). See, Configuring the Amazon WorkSpaces broker connection.
- Added the INI parameter for connecting AWS using the registration code. See, Configuring the Amazon WorkSpaces broker connection.

#### · Cisco Jabber updates

Supports JVDI audio calls on Wyse 5010, 5040 AlO, and 3030 LT thin clients. See, Cisco Jabber Softphone for VDI.

#### · PCoIP updates

Supports customizing the PCoIP connection broker window and icons. See, Customize connection broker agent window and icons.

Network updates

Supports onboard Ethernet port, Ethernet port on the docking station, and wireless on the Wyse 5470 Thin Client. See, Configuring connectivity.

#### ThinOS enhancements

- Added the Korean language option in the Locale drop-down list. See, Configuring the system preferences.
- o Supports the word wrap feature using the INI parameter. See, Word wrap feature.
- Changes to the close lid behavior on the Wyse 5470 Thin Client. For more information, see the Dell Wyse ThinOS 8.6 INI Reference Guide and Dell Wyse ThinOS 8.6 Operating System Release Notes at www.dell.com/support.

#### INI updates

New INI parameters are added in this release. For more information, see the *Dell Wyse ThinOS 8.6 INI Reference Guide* at www.dell.com/support.

# What is new in ThinOS 8.6\_027

The following are the new features or updates to the existing features in this release:

- · Updates to ThinOS packages
  - o Updated the Citrix RTME package to version 2.8.
  - Updated the VMware Horizon package to version to 5.1.
  - Updated the Flash Redirection package to version 1.28.
- VMware updates
  - Updated the VMware Horizon client from version 5.0 to version to 5.1.
  - o Supports the relative mouse feature in a Blast session. See, Enable relative mouse feature.
  - o Supports USB splitting for Blast protocol. See, USB device splitting in Blast session.
- Imprivata updates
  - o Added grace period support to skip the second authentication factor. See, Grace period to skip second authentication factor.
- Amazon WorkSpaces updates
  - Supports Amazon WorkSpaces using direct connection mode. See, Configuring the Amazon WorkSpaces broker connection.
- ThinOS enhancements
  - o Supports the Omnikey 5321v2 device. See, Smart cards and smart card readers.
  - o Supports Rutoken smart cards. See, Rutoken smart card reader
  - $\circ \quad \text{Added the option to disable on-board serial ports using INI parameters. See, Configuring the serial settings.}\\$
  - o Improved the security for CA validation on Wyse Management Suite. See, Configuring the Wyse Device Agent settings.

#### INI parameter updates:

Added new INI parameters. See, Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/manuals.

# What is new in ThinOS 8.6\_024

The following are the new features or updates to the existing features in this release:

#### Updates to ThinOS packages:

- Updated the VMware Horizon package to version 5.0.53374.
- Updated the Flash Redirection package to version 1.26.53224.

#### VMware updates:

- Updated the VMware Horizon package version from 4.8 to 5.0.
- Supports the relative mouse feature in a PCoIP session. See, Enable relative mouse feature.
- o Supports the High Color Accuracy feature in a Blast session with H.264 enabled. See, Global Connection Settings.
- Supports the Username Hint option during smart card authentication for the Horizon View broker. See, Enable username hint for smart card login.
- Enhanced the reconnect workflow for VMware Horizon View broker using INI parameters. See, Dell Wyse ThinOS Version 8.6 INI
  Reference Guide at www.dell.com/manuals.

#### · Teradici updates:

Supports the Teradici Cloud Access connection broker. See, Configuring Teradici Cloud Access.

#### · Imprivata updates:

Added support to treat smart card authentications as proximity card authentications. See, Use smart card as proximity card.

#### Enhancements:

- o UI enhancement to capture logs of the application console. See, Using the troubleshooting options.
- o UI enhancement to select DisplayPorts for DP audio. See, Configuring the audio settings.
- UI enhancement to display Frames Per Second (FPS) in the **Performance Monitor** window. See, Using the troubleshooting options.
- Supports creating a VDI connection by a low-privileged user using INI parameters. See, Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/manuals.
- Supports a new system variable—\$UMAC—for MAC address in the uppercase format. See, Dell Wyse ThinOS Version 8.6 INI
  Reference Guide at www.dell.com/manuals.
- Supports customizing the text color in the lock window using INI parameters. See, Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/manuals.

#### INI parameter updates:

Added new INI parameters. See, Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/manuals.

i NOTE: ThinOS 8.6\_024 supports Wyse Management Suite version 1.4.

# What is new in ThinOS 8.6\_019

The following are the new features or updates to the existing features in this release:

#### Updates to ThinOS packages:

- Updated the Citrix RTME package to version 2.7.52738. See, Citrix HDX RealTime Optimization pack.
- Updated the Cisco Jabber Softphone for VDI package to version 12.1.52977. See, Cisco Jabber Softphone for VDI.
- o Updated the VMware Horizon package to version 4.8.51817. See, Configuring VMware.

#### · Enhancements:

- Added the sleep mode feature that enables the power-saving state and quickly resumes full power operations without loss of data.
   This feature is supported on Wyse 5040 All-in-One client and Wyse 5040 All-in-One client with PCoIP. See, Sleep mode.
- Supports the VMware Blast Virtual channel on Imprivata Biometrics and Proximity devices. See, Imprivata Bio-metric Single Sign-On
- Supports User Datagram Protocol (UDP) through TS Gateway connections. See, Connect to RDP session using UDP with TS Gateway.
- $\circ\quad$  Supports the OMNIKEY 5422 smart card reader.
- o Supports SecMaker Net iD smart card. See, the Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/support.
- Supports disabling the cipher suites such as DES, 3DES or both for TLS clients. See, the Dell Wyse ThinOS Version 8.6 INI
  Reference Guide at www.dell.com/support.

#### INI parameter updates:

Added new INI parameters. See, the Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/support.

# What is new in ThinOS 8.6\_013

The following are the updates to the existing features or new features in this release:

#### · Citrix updates:

- Updated the Citrix RTME package to version 2.5. See, Citrix HDX RealTime Optimization pack.
- o Added support for Cisco Jabber Softphone for VDI. See, Cisco Jabber Softphone for VDI.
- Added support for Okta using Citrix NetScaler Gateway. See, Configuring Citrix NetScaler using Okta.
- Added support to create icon folders on the StoreFront desktop using the INI parameter. See, the Dell Wyse ThinOS Version 8.6
   INI Reference Guide at www.dell.com/support.
- o Added support for multiple logins with Citrix and VMware Horizon. See, Multiple logins with Citrix and VMware Horizon.

#### VMware updates:

- Updated the Horizon client version from 4.6 to 4.8. See, Configuring VMware.
- Added support for VMware Horizon Virtualization Pack for Skype for Business in VMware Blast session. See, VMware Horizon Virtualization Pack for Skype for Business.
- o Added support for hardware cursor in VMware Blast session. See, Enable hardware cursor in Blast session.
- Added support for multiple logins with VMware Horizon and Citrix. See, Multiple logins with Citrix and VMware Horizon.

#### RDP updates:

- o Ability to select displays when launching RDP connections in full screen mode. See, Configuring RDP connections.
- o Added an option to set the desktop DPI scaling factor. See, Global connection settings.

#### PCoIP updates:

Added support to directly configure the PCoIP connection using Teradici Remote Workstation cards. See, Configuring PCoIP connections using Teradici Remote Workstation card.

#### BIOS updates:

- Added support to update BIOS on Wyse 5060 and 3030 LT thin clients using Wyse Management Suite. See, Upgrading BIOS on Wyse 5060 thin client and Wyse 3030 LT thin client.
- Added support to extract and restore certain BIOS settings. See, Using the troubleshooting options.

#### Enhancements:

- o UI enhancement to configure the IPv4 settings for a wireless connection. See, Configure the WLAN settings.
- UI enhancement to enable user to connect to a remote host or device using the Telnet client. See, Using the troubleshooting
  options.
- o UI enhancement to verify the version of the installed packages and generate logs. See, Accessing system information.
- o UI enhancement on the Wyse Device Manager console to display the device details of peripheral devices that are connected to the ThinOS client. For more information, see the *Dell Wyse Device Manager Administrator's Guide* at www.dell.com/support.
- o Added support for Caradigm Way2Care. See, Caradigm Way2Care enhancement.
- Added support for Vertical Synchronization to eliminate screen tearing. See, Vertical Synchronization.
- o DisplayPort audio is disabled by default on Wyse 3040 thin client.
- Only 32-bit desktop color is supported on Wyse 3010 thin client and Wyse 3020 thin client.
- o Monitor priority is modified for Wyse 5070 Extended thin client. See, Hardware capability.

#### INI parameter updates:

Added new INI parameters. See, Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/support.

# Before working on ThinOS

This section contains information about firmware upgrade and system configuration that you need to know before using ThinOS version 8.6

# Firmware upgrade and package deployment

Consider the following before you upgrade the ThinOS firmware and deploy the ThinOS packages:

- On Wyse 5070 Extended thin client, the AMD firmware is upgraded to a newer version. If you want to downgrade ThinOS from 8.6 to 8.5.1, you must shut down and boot the thin client again. If you do not shut down and reboot, a black screen is displayed on the monitor that is connected to the AMD GPU port. Also, the AMD DP port sequence is updated.
- On Wyse 5070 thin clients, the Bluetooth firmware is upgraded to a newer version from ThinOS 8.5\_108. If you want to update the thin client with the Bluetooth module from ThinOS version 8.5\_107 to 8.5\_108 or later, Dell recommends that you disconnect the power cable and connect the power cable again before you reboot.
- In ThinOS 8.6, the installed RTME, Horizon, and JVDI packages are saved to the hidden partition. When you downgrade ThinOS firmware to previous versions, and upgrade the firmware to 8.6 again, the ThinOS device reinstalls the saved packages from the hidden partition. You can delete the package to clean the backup data from the device.
- · From ThinOS version 8.6, the Merlin images include both RTME and Horizon packages.
- · If you push Merlin images on Wyse 5010, 5040, and 7010 thin clients with 4 GB or higher flash size, the RTME and Horizon packages are formatted.

To upgrade the ThinOS firmware, use any of the following:

- · HTTPS Windows server
- · Dell Wyse Management Suite

NOTE: To avoid uncertain issues, ensure that when you upgrade your firmware, you do not skip versions. To downgrade the ThinOS firmware, ensure that you set the INI parameter Autoload=2, and follow the procedure using the HTTPS server.

#### Table 1. Firmware images

Platform	ThinOS	ThinOS with PCoIP
Wyse 3020 Thin Client	T10D_wnos	Not available
Wyse 3030 LT 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	Not available
Wyse 5070 Thin Client—Celeron processor	X10_wnos	PX10_wnos
Wyse 5070 Thin Client—Pentium processor	X10_wnos	PX10_wnos
Wyse 5070 Extended Thin Client—Pentium processor	X10_wnos	PX10_wnos
Wyse 5470 Thin Client	X10_wnos	PX10_wnos
Wyse 5470 All-in-One Thin Client	X10_wnos	PX10_wnos

#### **Table 2. Package information**

Package name	Details
Base.i386.pkg	Automatically updated upon firmware upgrade.
Pcoip.i386.pkg	Automatically updated upon firmware upgrade of a PCoIP client.
RTME.i386.pkg	Upload the new package to central configuration, and system can update without INI configuration.
Horizon.i386.pkg	Upload the new package to central configuration, and configure the INI parameter to update this package.
JVDI.i386.pkg	Upload the new package to central configuration, and configure the INI parameter to update this package.

#### (i) NOTE:

- When the packages fail to update, or cannot function after update with new version firmware, or if there is further failure, the workaround is to remove all packages and reinstall the packages upon reboot.
- For information about the ThinOS build number, and package versions, see the latest *Dell Wyse ThinOS Release*Notes.

# Firmware upgrade using HTTPS

Ensure that you have set up a Windows PC or Server with Microsoft Internet Information Services (IIS) and HTTPS services installed. If you do not have the HTTPS server installed, then refer to the article about how to setup an HTTPS server at support.microsoft.com.

Ensure that the web server can identify the file types used by ThinOS. Create two MIME types under IIS. The MIME's option needs to be configured on a per site basis. On a default IIS, install:

- 1. Launch the IIS admin console.
- 2. Browse to the default website, right-click and select **Properties**.
- 3. Click the HTTP Headers tab, and in the MIME Map section, select File types > New Type.
- 4. Add the two MIME types. Use .INI and . for the associated extension fields.
- 5. Apply the settings and close the IIS admin console.

Installing IIS creates the default directory C:\inetpub\WWWroot, which is known as the WWW root. In the WWWroot directory, create a folder WYSE and a sub folder wnos. The directory structure must read as C:\inetpub\wwwroot\WYSE\wnos.

To upgrade the ThinOS firmware using HTTPS server:

- 1. Go to www.dell.com/support.
- 2. Download the latest ThinOS firmware and latest ThinOS packages that corresponds to your thin client model. If the firmware and packages are in the form of a compressed self-extracting (.EXE) or zipped file (.ZIP), then extract the files. When you download the JVDI.zip package, the README WITH EULA.txt and JVDI.i386.pkg files are unzipped. Ensure that you open the readme file and read the EULA agreement.
- **3.** Place the extracted firmware files in the C:  $\inetpub\wwwroot\WYSE\wnos$  folder, and the packages to C:  $\inetpub\wwwroot\WYSE\wnos\pkg$  on your HTTPS server.
- **4.** Create a wnos.ini text file (using a text editor) in the C:\inetpub\wwwroot\WYSE\wnos folder with the following INI parameters: Autoload=2 loadpkg=1 Addpkg=horizon, JVDI
  - NOTE: JVDI package is introduced from ThinOS version 8.6 to support Cisco Jabber. However, if you intend to use only horizon package, then do not load the JVDI package to avoid unknown user trap issue.

The option Autoload=2, ensures that the thin client uses the firmware installed on the server to upgrade, only if the firmware on the thin client is older than the version on the server. The option LoadPkg specifies how to update the external packages. If LoadPkg is not in the statement, it will inherit the value of AutoLoad.

Base package and the PCoIP package are integrated into the ThinOS firmware image. Installing the latest ThinOS firmware image automatically installs the latest version of these packages on the ThinOS client. If you set AutoLoad=1 LoadPkg=0, the firmware is checked, but the packages are not checked. The packages check is performed after firmware check. From ThinOS 8.3, the external packages update mechanism is changed. Some packages are default, and loaded according to value of LoadPkg. For example RTME. Some packages need additional parameter AddPkg to add. For example, Horizon and JVDI. The option AddPkg is for adding

packages. It depends on the value of LoadPkg. For more information about the INI parameter usage, see *Dell Wyse ThinOS INI* Reference Guide.

- 5. Save the wnos.ini file.
- 6. On the ThinOS client desktop, navigate to System Setup > Central Configuration > General.
- 7. In the General tab, enter the IP address of the file server or directory. For example: https://IPaddress/wyse.
  - NOTE: You can also use DHCP option tags 161 and 162 to configure the ThinOS client, file server and path information. You must create these options on your DHCP server, configure them with the correct server information, and enable the DHCP server scope in your environment.
- 8. Click OK.
- 9. Restart the thin client and wait until the auto-installation of packages is complete.

## Firmware upgrade using Wyse Management Suite

Ensure that you have created a custom group and assigned the ThinOS devices to that group in Wyse Management Suite—see Dell Wyse Management Suite Administrator's Guide.

Ensure that your ThinOS clients are registered to Wyse Management Suite.

To upgrade the ThinOS firmware using Wyse Management Suite:

- 1. Go to www.dell.com/support.
- 2. Download the latest ThinOS firmware and ThinOS packages that corresponds to your thin client model. When you download the JVDI.zip package, the README WITH EULA.txt and JVDI.i386.pkg files are unzipped. Ensure that you open the readme file and read the EULA agreement.
  - NOTE: JVDI package is introduced from ThinOS version 8.6 to support Cisco Jabber. However, if you intend to use only horizon package, then do not load the JVDI package to avoid unknown user trap issue.
- 3. Log in to Wyse Management Suite using valid credentials.
- 4. On the Apps & Data page, in the OS Image Repository section, click ThinOS.
- 5. Click Add Firmware File.
  - The Add File dialog box is displayed.
- 6. Browse and select the downloaded firmware file. Enter an appropriate description.
- 7. Click Upload.
  - The ThinOS firmware file is uploaded, and the firmware file is listed on the Apps & Data ThinOS OS Image Repository page.
- 8. Select the check box that corresponds to your ThinOS firmware file.
- On the Groups & Configs page, select a custom group, and click Edit Policies > ThinOS.
   The Select ThinOS Configuration Mode screen is displayed.
- 10. Click Advanced Configuration.
- 11. In the Device Configuration pane, click Firmware Upgrade, and then click Configure this item.
- 12. From the **Platform type** drop-down list, select your thin client model.
- 13. From the Firmware to auto deploy drop-down list, select the firmware file that corresponds to your thin client model.
- 14. Click Save & Publish.

The thin client restarts, and the firmware version is upgraded.

# Firmware installation using Dell Wyse USB Imaging Tool

Use the Dell Wyse USB Imaging Tool version 3.1.0 to install the ThinOS merlin image on your thin client. For information about installation instructions, see the Dell Wyse USB Imaging Tool version 3.1.0 User's Guide at downloads.dell.com/wyse/USBFT/3.1.0/.

# **BIOS upgrade**

BIOS upgrade is the process of updating your existing BIOS version to the latest version.

#### Table 3. BIOS binary files

Platform	BIOS binary filename
Wyse 3020 thin client	Not available
Wyse 3030 LT thin client	U10_bios.bin
Wyse 3030 LT thin client with PCoIP	PU10_bios.bin
Wyse 3040 thin client	A10Q_bios.bin
Wyse 3040 thin client with PCoIP	A10Q_bios.bin
Wyse 5010 thin client	D10G_bios.bin
Wyse 5010 thin client with PCoIP	PD10G_bios.bin
Wyse 5040 AIO thin client	AIO10G_bios.bin
Wyse 5040 AIO thin client with PCoIP	PAIO10G_bios.bin
Wyse 5060 thin client	D10Q_bios.bin
Wyse 5060 thin client with PCoIP	PD10Q_bios.bin
Wyse 7010 thin client	Z10G_bios.bin
Wyse 5070 thin client-Celeron	X10_bios.bin
Wyse 5070 thin client-Pentium	X10_bios.bin
Wyse 5070 Extended thin client	X10_bios.bin

When you use a file server to update BIOS for Wyse 5060 and 3030 LT thin clients, the BIOS update progress bar disappears after the BIOS update process is complete, and the system reboots after one minute. You must not manually reboot the thin client. During reboot, a black screen is displayed for one minute, and then the device resumes the BIOS update.

NOTE: For information about the BIOS versions, see the latest *Dell Wyse ThinOS Release Notes* 

# Upgrading BIOS on Wyse 5060 thin client and Wyse 3030 LT thin client

This section describes the procedure to update BIOS on Wyse 5060 thin client with ThinOS, and Wyse 3030 LT thin client by using Wyse Management Suite version 1.3.

- Download the Dell BIOS file at www.dell.com/support.
   For example, Wyse\_5060\_version.bin. The BIOS version may be updated in each release. For the latest version of BIOS, see the latest Dell Wyse ThinOS Release Notes.
- 2. Log in to Wyse Management Suite.
- 3. Click Apps & Data.
- 4. In the OS Image Repository section, click ThinOS.
- 5. Click Add BIOS file.
  - The Add File screen is displayed.
- 6. To select a BIOS file, click **Browse** and navigate to the location where your BIOS file is located.
- 7. Enter the description for the BIOS file.
- 8. If you want to override an existing BIOS file, select the Override existing file check box.
- 9. From the BIOS platform type, select either Wyse 5060 thin client or Wyse 3030 LT thin client based on your device type. You can also select multiple platforms.
- 10. Click Upload.
  - NOTE: The BIOS file is added to the repository. However, the BIOS file is not assigned to any groups or devices. You must make assignments on the Device Configuration page.
- 11. Click Groups & Configs.
- 12. Select a group, and click Edit Policies.

13. Click ThinOS

The Select ThinOS Configuration Mode window is displayed.

- 14. Click Advanced Configuration.
- 15. In the Device Configuration section, click Firmware Upgrade.
- 16. Select the Enable BIOS Upgrade check box.
- 17. Select one or more BIOS files.

#### (i) NOTE:

- When deploying a group policy, you can select multiple BIOS files. However, the policy must reject any duplicate platforms.
- If two BIOS files are selected, the policy cannot be saved and an error Firmware Upgrade policy contains
  duplicate platforms for BIOS upgrade is displayed.
- At Device Level Exception, only BIOS files that have the same platform as the selected device are listed. You can select only a single file.

#### 18. Click Save & Publish.

If BIOS is already applied, the ThinOS client ignores the BIOS update process. If the BIOS version of the uploaded file does not match the existing BIOS version on the thin client, the BIOS file is successfully downloaded and updated on the thin client.

## **Upgrading BIOS on Wyse 3040 thin client**

This section describes the procedure to update BIOS on Wyse 3040 thin client with ThinOS, and Wyse 3040 thin client with PCoIP by using file server.

The Dell Standard BIOS file is converted to BIN file format for signature and security purposes. The format of the BIN file is  $Wyse_3040\_version.bin$ .

#### Upgrading BIOS by using file server

To upgrade BIOS using file server, do the following:

- Download the Dell BIOS file at the www.dell.com/support.
   For example, Wyse\_3040\_version.bin. The BIOS version may be updated in each release. For the latest version of BIOS, refer to the latest Dell Wyse ThinOS Release Notes.
- 2. Rename the Dell BIOS file as A10Q bios.bin.
- ${\bf 3.}\ \ \, {\rm Upload}$  the renamed BIOS file to folder WNOS in the https server.
- 4. Ensure that the INI parameter autoload is enabled for firmware update in WNOS.INI.
- **5.** Restart the thin client. BIOS is updated automatically.

To verify whether the new BIOS is updated correctly, from the desktop menu, click the **System Information** option, or click the **System Information** icon in zero mode. In the **Event Log** tab, the BIOS version log is displayed.

For example, System Version: 8.5\_017 (ROM 1.2.1).

This log indicates that the BIOS version is updated to  $\lor$ 1.2.1.

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

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

The BIOS version is displayed on the screen.

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

# Upgrading BIOS on Wyse 5070 thin client

This section describes the procedure to update BIOS on Wyse 5070 thin client with ThinOS, and Wyse 5070 thin client with PCoIP by using file server. The Dell Standard BIOS file is converted to BIN file format for signature and security purposes. The format of the BIN file is Wyse 5070 version.bin.

To upgrade BIOS using the file server:

- Download the Dell BIOS file from the Dell support site.
   For example, Wyse\_5070\_1.0.3.bin. The BIOS version may be updated in each release. For the latest version of BIOS, see the latest Dell Wyse ThinOS Release Notes.
- 2. Rename the Dell BIOS file as X10 bios.bin.
- **3.** Upload the renamed BIOS file to folder WNOS in the https server.
- 4. Ensure that the INI parameter autoload is enabled for firmware update in WNOS.INI.
- **5.** Restart the thin client. The BIOS is updated automatically.

To verify whether the new BIOS is updated correctly, from the desktop menu, click the **System Information** option, or click the **System Information** icon in zero mode. In the **Event Log** tab, the BIOS version log is displayed.

For example, **System Version: 8.5\_108—ROM 1.0.3**.

This log indicates that the BIOS version is updated to v1.0.3.

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

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

The BIOS version is displayed on the screen.

BIOS can also be updated by using the Wyse Management Suite version 1.2 console. For more information about Wyse Management Suite, see *Dell Wyse Management Suite Administrator's Guide*.

## **Upgrade BIOS on the Wyse 5470 Thin Client**

This section describes the procedure to update BIOS on the Wyse 5470 Thin Client by using file server. The Dell Standard BIOS file is converted to BIN file format for signature and security purposes. The format of the BIN file is  $5470\_bios.bin$  for Wyse 5470 Thin Client.

To upgrade BIOS using the file server:

- Download the Dell BIOS file from the respective hardware pages on Dell support site.
   For example, 5470\_bios.bin. The BIOS version may be updated in each release. For the latest version of BIOS, see the latest Dell Wyse ThinOS Release Notes.
- 2. Upload the BIOS file to folder WNOS in the https server.
- 3. Ensure that the INI parameter autoload is enabled for firmware update in WNOS.INI.
- **4.** Restart the thin client.

The BIOS is updated automatically.

To verify whether the new BIOS is updated correctly, from the desktop menu, click the **System Information** option, or click the **System Information** icon in zero mode. In the **Event Log** tab, the BIOS version log is displayed.

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

- 1. Restart the thin client, and during system boot, press the  ${\bf F2}$  key.
- 2. Enter the BIOS password, if admin password is set.
- 3. Click Settings > General > System Information.

The BIOS version is displayed on the screen.

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

## Upgrade BIOS on the Wyse 5470 All-in-One Thin Client

This section describes the procedure to update BIOS on the Wyse 5470 All-in-One Thin Client by using file server. The Dell Standard BIOS file is converted to BIN file format for signature and security purposes. The format of the BIN file is 5470AIO\_bios.bin for the Wyse 5470 All-in-One Thin Client.

To upgrade BIOS using the file server:

Download the Dell BIOS file from the respective hardware pages on Dell support site.
 For example, 5470AIO\_bios.bin. The BIOS version may be updated in each release. For the latest version of BIOS, see the latest Dell Wyse ThinOS Release Notes.

- 2. Upload the BIOS file to folder WNOS in the https server.
- 3. Ensure that the INI parameter autoload is enabled for firmware update in WNOS.INI.
- **4.** Restart the thin client. The BIOS is updated automatically.

To verify whether the new BIOS is updated correctly, from the desktop menu, click the **System Information** option, or click the **System Information** icon in zero mode. In the **Event Log** tab, the BIOS version log is displayed.

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

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

The BIOS version is displayed on the screen.

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

# System configuration and deployment

- USB redirection must be disabled for audio and video devices to use RTME, RTAV, SFB, and JVDI. By default, the USB redirection is
  disabled on ThinOS. Dell recommends that you do not modify the default settings unless you need the USB redirection for audio and
  video devices.
- ThinOS BIOS policy can be configured using Wyse Management Suite Console, Wyse Management Suite group INI, and Wyse Management Suite advanced settings. Dell recommends that you use any one of the methods to configure the BIOS policy. Setting the BIOS policy simultaneously using different methods may cause a policy mismatch, and the device reboots repeatedly. This reboot loop issue is observed when you select the **reboot immediately** option in the **BIOS policy** settings section on the Wyse Management Suite console.
- All the installed packages are deleted when you update the ThinOS image version between major releases using WDM or Wyse Management Suite.

**Solution for updating firmware using WDM**—Ensure that you have set the PKG install parameters in the WNOS.ini, and the pkg files are uploaded in the directory. After the device reboot, the packages are re-installed automatically.

**Solution for updating firmware using Wyse Management Suite**—Wyse Management Suite App policy works only once after the policy is created. The deleted package cannot be reinstalled using the same policy. Dell recommends that you create a new App policy to install the package after the firmware update is complete.

- WDM vulnerability is fixed in this release. You must configure either the DHCP or the DNS option/record of the WDM server
  fingerprint to automatically fetch and validate the fingerprint before checking in to the WDM server. However, there is no impact to
  the ThinOS device functionality if you do not to configure the fingerprint validation environment. For more information about how to
  set up fingerprint using WDM, see How to set up WDM fingerprint using Wyse Device Manager.
- · Boot up unit without monitor or with monitor power-off.
  - Wyse 5010 thin client, Wyse 5040 thin client, Wyse 7010 thin client, and Wyse 3030 LT thin client—If the thin client waits for 15 to 20 seconds and the monitor is attached or powered on within 20 seconds, the display is turned on. If the monitor is attached or powered on after 20 seconds, the monitor displays the black screen. Turn on the monitor first, and then turn on the thin client.
  - o Wyse 3040 thin client and Wyse 5060 thin client: The client waits until the monitor is attached or turned on.

## How to set up fingerprint using Wyse Device Manager

To set up your fingerprint using WDM, do the following:

- 1. Export the WDM server certificate from the WDM server that you want to access.
- 2. Extract the fingerprint value from the WDM certificate in the required format.

You must use a system with OpenSSL installed. OpenSSL can be used to extract the fingerprint in required format from the WDM certificate itself.

The fingerprint is generated from the following command:

openssl x509 -in <your certificate name>.crt -pubkey -noout | openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64

- NOTE: If cert.crt is in DER format instead of the PEM format, you must add -inform to the first command. The certificate supports SHA256 in base64 encoded format.
- 3. Configure either the DHCP option or the DNS TXT record.
  - · If you want to use the DHCP option, configure the following option tags defined in the DHCP server:
    - o Option ID—200
    - o Name—WDM\_Fingerprint
    - o Type—String
  - · If you want to use the DNS TXT record, enter the name as WDM\_Fingerprint, and provide the fingerprint string value.
- NOTE: If the DNS TXT record for fingerprint cannot be retrieved, the device fetches the values from the DHCP scope option. If the fingerprint certificate is already available, the device checks in to the WDM server. If the connection fails, the failure logs are registered on the ThinOS client.

# Automating updates and settings using central configuration

ThinOS is centrally managed and configured using INI files to automatically push updates and any desired default configuration to thin clients in your environment. This section describes how to set up your environment to provide your thin clients running ThinOS with automatic updates and configurations in three simple steps. If no INI files are detected, you can use local dialog boxes on each thin client to configure the settings. Many of these locally configured settings such as resolution, mouse, and keyboard are saved on ThinOS to persist after reboot. However, once INI files are detected, rebooting the client causes ThinOS to become stateless, and ignores the locally configured settings after a reboot. The settings contained in the INI file are used.

NOTE: Dell Wyse thin clients do not require device management software. They are configured to obtain their IP address, as well as the location of firmware and configuration instructions, from a DHCP server. However, you can use Wyse Device Manager (WDM) or Wyse Management Suite for a more hands-on management of your thin clients. For information about configuring your thin clients to communicate with a WDM server or Wyse Management Suite, see the related INI parameters in *Dell Wyse ThinOS INI Guide*.

## How to set up automatic updates and configurations

For a thin client running ThinOS to successfully access INI files and update itself from a server, you must set up the server with the correct folder structure where the INI files and other update files are located, direct the thin client to the server, and then reboot or start the thin client

Once DHCP and servers are configured and available, the thin client checks (at each boot up) to see whether or not any updates are available on a predefined server DHCP Option #161 specifies the server URL, DHCP Option #162 specifies the root path to the server. If updates are available, the updates are automatically installed.

## **Using DHCP options**

This table contains the DHCP options available for use.

#### Table 4. DHCP options

Option	Description	Notes
1	Subnet Mask	Required. However, it is not required unless the thin client must interact with servers on a different subnet. MS DHCP requires a subnet mask and is always send one.
2	Time Offset	Optional.
3	Router	Optional, but recommended. It is not required unless the thin client must interact with servers on a different subnet.

Table 4. DHCP options (continued)

Description	Notes
Domain Name Server (DNS)	Optional, but recommended.
Domain Name	Optional, but recommended. See Option 6.
Broadcast Address	Optional.
WINS servers IP Address	Optional.
Lease Time	Optional, but recommended.
Option Overload	Optional.
DHCP Message Type	Recommended.
DHCP Server IP Address	Recommended.
Parameter Request List	Sent by thin client.
Maximum DHCP Message Size	Optional (always sent by thin client).
T1 (renew) Time	Optional, but recommended.
T2 (rebind) Time	Optional, but recommended.
Client identifier	Always sent.
File server (https)	Optional string. Can be either the name or the IP address of the file server. If a name is given, the name must be resolvable by the DNS servers specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to also be the file server.
Root path to the file server (https)	Optional string. If the option provided by the server is blank and the server provides no value for the field, a null string is used.  \mathbb{\text{wyse}\mathbb{\mathbb{w}} nos is automatically appended to the search path. For example, if you enter pub\serversoftware, the path searchedare pub\serversoftware\mathbb{\mathbb{w}} nos.  i NOTE: You can have the \mathbb{\mathbb{w}} searched path omitted by appending a dollar sign (\$) to the entered path. For example, if you enter pub\serversoftware\\$, the path searched will be pub\serversoftware\\$ wnos.  i NOTE: The usage or omission of a leading slash (\) on the path is critical on some servers. Some servers limit access to the root path of the user specified at login. For those servers, the usage of the leading slash is optional. Some  *NIX servers can be configured to
	Domain Name Server (DNS)  Domain Name  Broadcast Address  WINS servers IP Address  Lease Time  Option Overload  DHCP Message Type  DHCP Server IP Address  Parameter Request List  Maximum DHCP  Message Size  T1 (renew) Time  T2 (rebind) Time  Client identifier  File server (https)

Table 4. DHCP options (continued)

Option	Description	Notes
		entire file system. For those servers, specifying a leading slash specifies that access is to start at the root file system. Proper matching of the file specification to the file server in use is critical to ensuring proper operation. A secured Windows server requires the slash to be specified in order to complete proper access.
165	WMS Server	Optional string. Specifies the IP address of the Wyse Management Suite Server.
166	WMS MQTT Server	Optional string. Specifies the IP address of the MQTT Server.
167	WMS CA Validation	Optional string.
181	PNAgent/ PNLite server list	Optional string. The thin client uses the server to authenticate the Windows credentials of the user and to obtain a list of ICA published applications valid for the validated credentials. The user supplies those credentials when logging in to the thin client.
182	NT domain list for PNAgent/ PNLite	Optional string. The thin client creates a pull-down list of domains from the information supplied in option 182. This list is presented at thin client login in the order specified in the DHCP option (for example, the first domain specified becomes the default). The selected domain is the one which must authenticate the user ID and password. Only the selected domain is used in the authentication process. If the domain list is incomplete and the user credentials must be verified against a domain not in the list, assuming that the server in option 181 is capable of authenticating against a domain not in the list, the user has the option of not using any of the domains specified in option 182 and typing a different domain name at the time of login.
184	File server Username	Optional string. Username to use when authenticating to the server specified in Option 161.
185	File server Password	Optional string. Password to use when authenticating to the server specified in Option 161.
186	WDM server list	Optional binary IP addresses of WDM. This option can specify up to two WDM servers. If two are specified, at boot time the thin client attempts to check-in to the first server. If it cannot contact the first server, it tries to check-in to the second server.

Table 4. DHCP options (continued)

Option	Description	Notes
187	WDM server port	Optional number. Byte, word, or two-bytes array.  (i) NOTE: The value of this option tag, when not embedded in Vendor Class Specific Information option, is interpreted in reverse order when it is sent as 2-bytes example, the value of 0x0050 was interpreted as 0x5000. This option tag was used by old ThinOS releases. New ThinOS releases still accept this option tag for backward compatibility.
188	Virtual Desktop Broker server	Optional string.
190	WDM secure port	Optional number, word or two-bytes array. Specifies to use HTTPS to communicate with WDM instead of HTTP.
192	WDM server port	Optional number, word or two-bytes array.  (i) NOTE: The value of this option tag represents the same information as option tag 187. The difference is that ThinOS interprets the value of this option tag in correct order (for example, the value of 0x0050 is interpreted as0x0050). If the DHCP server provides both option tag 192 and 187, option tag 192 takes precedence.
194	WDM FQDN	Optional Fully Qualified Domain Name for the WDM.
199	Wyse Management Suite Group Key	Optional string. Can provide a Wyse Management Suite Group Registration Key for the Wyse Management Suite agent. When Wyse Management Suite is disabled and the Group Key of Wyse Management Suite is null, this option takes effect. Wyse Management Suite uses the optional string as the Group Registration Key. If the Wyse Management Suite server or MQTT server is null, the Wyse Management Suite server values.

# **Getting started**

This chapter helps you quickly learn the basics and get started with your thin client.

# **End User License Agreement**

End User License Agreement is added to ThinOS from this release. End User License Agreements must be read and accepted to continue using ThinOS. The End User License Agreement screen is displayed during the following instances:

- · When you boot the thin client for the first time.
- · When you reset a thin client that runs ThinOS version 8.5 or later, to factory settings.
- NOTE: If the thin client is managed using Wyse Management Suite server, the End User License Agreement screen is not displayed.

# Configuring ThinOS using the First Boot Wizard

The First Boot Wizard runs the first time you start a new thin client with ThinOS. The thin client starts the First Boot Wizard application before you enter the ThinOS system desktop, and allows you to perform a set of tasks, such as, configuring system preferences, setting up the internet connectivity, loading USB configurations, configuring management software, and configuring broker connections.

If you are an existing thin client user, and you have upgraded to the ThinOS version 8.5 or later, then you can reset your thin client to factory default settings to enter the First Boot Wizard.

To configure the First Boot Wizard:

- 1. Connect a new thin client or existing thin client to the Ethernet using a wired connection. The existing thin client must be reset to factory default settings to enter the First Boot Wizard.
- 2. Turn on your thin client.

The thin client checks for a wired network connection. If the network connection is successful, a welcome screen with the model name of your thin client and the End User License Agreement screen is displayed. For more information, see End User License Agreement.

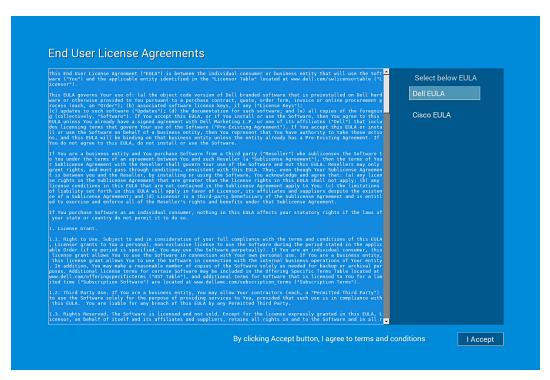


Figure 1. Dell EULA

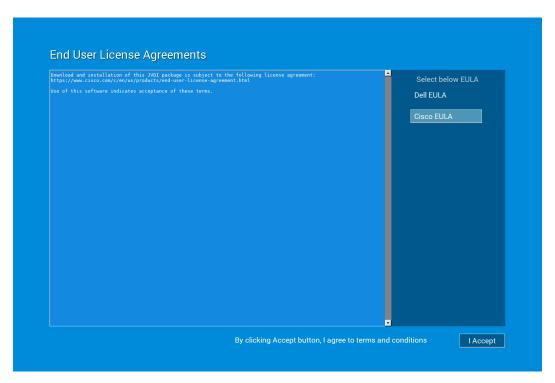
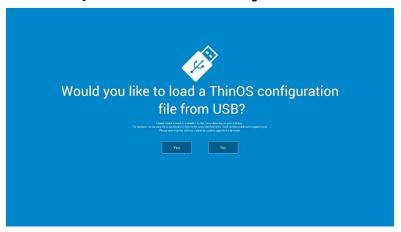


Figure 2. Cisco EULA

- 3. Select **Dell EULA** and **Cisco EULA** from the right pane to read both the End User License Agreements.
  - NOTE: Cisco End user Agreement is displayed only if you have the JVDI package installed.
- 4. Accept each End User License Agreement by clicking I Accept .

The thin client validates the IP address from DHCP. If the DHCP contains the file server or the Wyse Device Manager or Wyse Management Suite configurations, then the ThinOS system desktop is loaded without entering the First Boot Wizard. If the DHCP validation fails or if you have not connected to Ethernet, then follow the next step.

- NOTE: To exit the First Boot Wizard during the network connection status check on the welcome screen, press the Ctrl + Esc key.
- 5. On the Would you like to load a ThinOS configuration file from USB? screen, do either of the following:



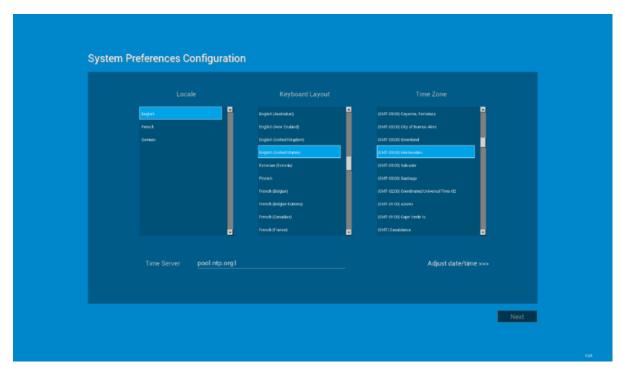
- To load a ThinOS configuration file from the USB drive, ensure that you create a wnos.ini file and add the file to the /wnos directory on the USB drive. Using this option, you can load packages, and wallpapers that are specified in the INI file. Plug in the USB drive to thin client, and click **Yes**.
  - NOTE: Only FAT, FAT32, and ExFAT file systems on the USB disk are supported. NTFS file system is not supported.

The thin client validates the configuration file in the USB drive.

- If the ThinOS configuration file in the USB drive is correct, the Read configuration success message is displayed. Click OK
  to exit the First Boot Wizard, and log in to the ThinOS system desktop.
- If the ThinOS configuration file in the USB drive is corrupted or the appropriate file is not available, then the Cannot find configuration files, or read configuration failure message is displayed. Upload the correct file on the USB drive, plug the USB drive again, and then click Retry. If the file is correct, the Read configuration success message is displayed. Click OK to exit the First Boot Wizard, and log in to the ThinOS system desktop.

If you do not want to use the **Retry** option to load the ThinOS configuration file, then click **Abort** to enter the **System Preferences configuration** setup.

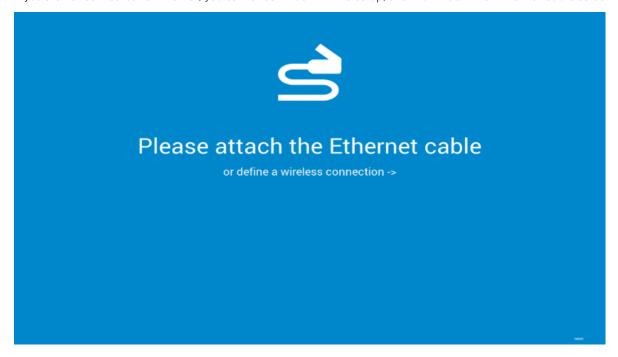
- NOTE: To exit the Cannot find configuration files, or read configuration failure message screen, and load the ThinOS system desktop, click Exit.
- · To enter the **System Preferences configuration** setup, click **No**.
- **6.** On the **System Preferences Configuration** screen, configure the following options:



- · Locale—Select a language to start ThinOS in the regional specific language.
- · Keyboard Layout—Select a keyboard layout to set the keyboard layout in the regional specific language.
- Time Zone—Select a time zone to set the time zone for your thin client.
- · Time Server—Displays the IP addresses or host names with optional port number of time servers.
- · Advanced—Click Advanced to configure settings, such as daylight saving, time format, date format, and time servers.

i NOTE: To exit the System Preferences Configuration screen, and load the ThinOS system desktop, click Exit.

If you are not connected to Ethernet, you cannot continue with the setup, and the Attach the Ethernet cable screen is displayed.



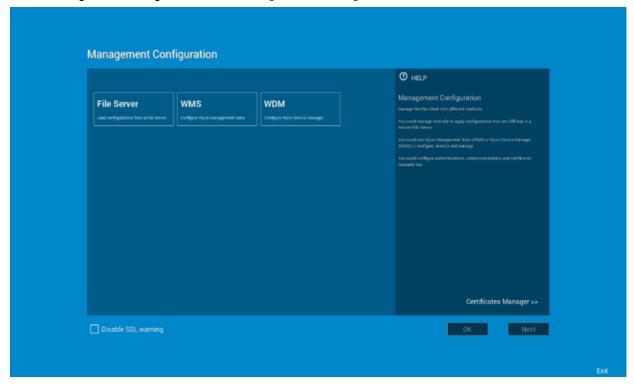
Do either of the following:

- · Connect the Ethernet cable to the thin client.
- · Click **Define a wireless connection**. From the list, select a wireless network, and click **Connect**.
  - (i) NOTE:

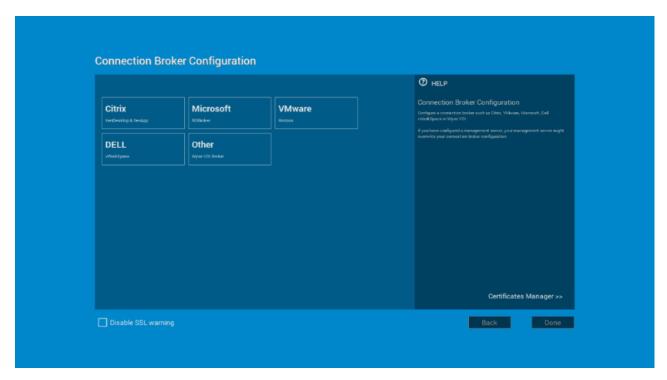
- o The option to define a wireless connection is not available on thin clients without a WLAN module.
- To exit the Attach the Ethernet cable screen, and load the ThinOS system desktop, click Exit.

After the connection is established, the thin client validates the IP address from DHCP. If the DHCP contains the file server or the Wyse Device Manager or Wyse Management Suite configurations, then the ThinOS system desktop is loaded. If the DHCP validation fails, or the network connection fails, then the **Management Configuration** screen is displayed. Follow steps 6–9.

- 7. Click Next to enter the Management Configuration setup.
- 8. On the Management Configuration screen, configure the following:



- · File Server—Enter the file server details to apply configurations including INI files, firmware, packages, and so on, from a file server
- **WMS**—Enter the group registration key and the Wyse Management Suite server URL to register the thin client to the Wyse Management Suite.
- · WDM—Enter the IP addresses or host names.
- · Disable SSL warning—Select this check box to disable the SSL (Secure Sockets Layer) connection warnings.
- · Certificates Manager—Click Certificates Manager to import or request a certificate.
- i NOTE: To exit the Management Configuration screen, and load the ThinOS system desktop, click Exit.
- 9. Click **Done** to exit the First Boot Wizard or click **Next** to enter the **Connection Broker Configuration** setup.
- 10. On the Connection Broker Configuration screen, configure the following:



- · Citrix—The broker allows you to connect to full desktops using Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) or individual applications using Citrix Virtual Apps (formerly Citrix XenApp) from a centralized host through Citrix Receiver Client.
  - Server Address—Enter the host name or IP address of the broker connection.
  - o Enable theme: ThinOS Lite—Select this check box to boot the thin client in ThinOS Lite mode.
  - StoreFront style—Select this check box to enable the Citrix StoreFront based layout of published applications and desktops on the thin client.
- Microsoft—The broker allows you to connect to the virtual desktops using RemoteApp and Desktop connection. Enter the host name or IP address of the broker connection.
- VMware—The broker allows you to connect to the remote desktops using VMware Horizon Client.
  - Server Address—Enter the host name or IP address of the broker connection.
  - Enable theme: VMware View—Select this check box to set the ThinOS desktop theme to VMware View mode.
- **DELL**—The broker allows you to connect to the virtual desktops or applications using Dell vWorkspace. Enter the host name or IP address of the broker connection.
- Amazon WorkSpaces—The broker allows your PCoIP clients to connect to virtual desktops that run on AWS. Enter the host name/IP address/FQDN of the broker connection.
  - i NOTE: Amazon WorkSpaces option is applicable only to the PCoIP clients.
- **Other**—The broker allows you to connect to the virtual desktops or applications using other supported protocols. Enter the host name or IP address of the broker connection.
- · Certificates Manager—Click Certificates Manager to import or request a certificate.
- · Disable SSL warning—Select this check box to disable the warnings for your SSL (Secure Sockets Layer) connection.
- 11. Click Done.
  - i NOTE: To configure the Management Configuration setup again, click Back, and follow steps 6 and 7.

The device exists from the First Boot Wizard mode, and the ThinOS desktop is displayed.

# Connecting to a remote server

On your initial connection to central configuration, we recommended that you connect using a **wired connection** plug in the network-connected Ethernet cable to your thin client before starting the thin client to obtain the configurations desired by the administrator. This **wired connection** will also provide any wireless configurations provided by the administrator through INI files.

If you must initially connect to central configuration through wireless, use the Wireless tab in the **Network Setup** dialog box to enter the SSID and encryption configurations required or set up by the network administrator. For more information, see Configuring the Network Settings.

**Central Configuration** — If you are configured for automatic detection using INI files — see *Dell Wyse ThinOS INI Guide*, your thin client will automatically detect and connect to the configured remote services during the boot-up process. Press the power button to turn on your thin client to see the **Login** dialog box. Enter your User name, Password, and Domain, and then click **Login**. After authentication is successful, your available connections are presented.

#### (i) NOTE:

Although the thin client will default to the Classic Desktop for INI backward compatibility, you can configure the thin client to display the Zero Desktop by using the SysMode=VDI parameter in the INI files or by selecting the desktop option in the dialog box. For more information, see Using Your Desktop.

**Manual Connection** — If you are not yet set up for central configuration, you will see the Zero Toolbar, where you can configure the initial server connection you want using the **Remote Connections** dialog box before you can log in. For more information, see Connecting to a Remote Server manually.

You only need to complete this manual configuration once or after reboot to factory defaults. After the thin client knows the location of your server, it automatically connects to the server for login when you start the thin client in the future. After you confirm that your environment is ready for deployment, you can create INI files for central configuration.

# Connecting a remote server manually

To connect a remote server manually, complete the following tasks:

- 1. Click the **System Settings** icon on the Zero Toolbar to open the System Settings menu, and then click **Remote Connections** to open the **Remote Connections** dialog box.
- 2. Click the **Broker Setup** tab of the **Remote Connections** dialog box to configure one of the following connections:
  - · ICA or RDP connection —Select None, select ICA or RDP, click Configure Connection, and then follow the wizard.
  - A specific broker server connection Select Microsoft, Citrix Xen, Dell vWorkspace, VMware View, Amazon WorkSpaces or Other, and then enter the IP Address for the server in the **Broker Server** box.
  - i NOTE: For more details, see Configuring the Remote Connections.
- 3. Click **OK**, and then restart the thin client.

Click the **Shutdown** icon on the Zero Toolbar to open, and use the **Shutdown** dialog box to restart the thin client.

#### (i) NOTE:

- If an ICA or RDP connection is configured— After thin client restarts, click the Home icon on the Zero Toolbar to open the list of available connections. Click the ICA or RDP connection you created, and then log in.
- If a specific Broker Server connection is configured— After thin client restart, the Login dialog box appears for your server. Enter the User name, Password, and Domain and click Login. After authentication is successful, your Zero Toolbar is presented with your assigned connections defined by the broker server.

# Using your desktop

What you see after logging on to the server depends on the administrator configurations.

- Users with a Classic Desktop—will see the classic ThinOS desktop with full taskbar, desktop, and Connect Manager familiar to
  ThinOS users. This option is the default out-of-the-box experience and is recommended for terminal server environments with
  published applications and for backward compatibility with ThinOS 6.x versions. For more information on using the Classic Desktop,
  see Classic Desktop Features.
- Users with a Zero Desktop—will see the Zero Desktop with the Zero Toolbar showing the assigned list of connections from which
  to select. This option is recommended for VDI and any full-screen only connections. For more information on using the Zero Desktop,
  see Zero Desktop Features.

In any desktop case, you can select the desktop option you want (Classic Desktop or Zero Desktop) and create the connections you need using the Visual Experience tab on the **Remote Connections** dialog box. To open the **Remote Connections** dialog box, perform one of the following tasks:

- Classic Desktop Click User Name, and then select System Setup > Remote Connections.
  - (i) NOTE: User Name is the user who is logged-on and is located at the lower-left pane of the taskbar
- · Zero Desktop Click the System Settings icon on the Zero Toolbar, and then select Remote Connections.

# Configuring thin client settings and connection settings

While the use of INI files is recommended to configure thin client settings and connection settings available to users, see How to set up automatic updates and configurations, you can use dialog boxes on a thin client to:

- · Set up your thin client hardware, look and feel, and system settings, see Configuring thin client settings locally.
- · Configure connection settings, see Configuring thin client settings locally.

# Connecting to a printer

To connect a local printer to your thin client, be sure you obtain and use the correct adapter cables which are not included. Before use, you may need to install the driver for the printer by following the printer driver installation instructions. For information on connecting to printers, see Configuring the printer setup.

# Connecting to a monitor

Depending on your thin client model, connections to monitors can be made using either a VGA (analog) monitor port, a DVI (digital) monitor port, or a DisplayPort (digital) and the proper Dell monitor cables/splitters/adapters.

#### (i) NOTE:

For dual-monitor supported thin clients— when using a DVI to DVI/VGA splitter, ensure that the DVI monitor will be the primary monitor; when using a DisplayPort, ensure that the DisplayPort monitor will be the primary monitor.

# Locking the thin client

To help ensure that no one else can access your private information without permission, ThinOS allows you to lock your thin client so that credentials are required to unlock and use the thin client after you do one of the following:

- **Unplug a signed-on smart card** If an administrator has set SCRemovalBehavior=1for the signing parameter in the INI files and you unplug the smart card that you used to sign on to the thin client, then the thin client will lock. To unlock the thin client for use, you must use the same smart card and your correct PIN. Note that removing a signed-on smart card can also cause the thin client to log-off, if an administrator has set the INI files to do so in this case you must sign-on as usual to use the thin client.
- Use Lock Terminal from the Shortcut Menu and Shutdown dialog box On the Classic Desktop, right-click on the desktop
  and select Lock Terminal, or use the Shutdown dialog box. On the Zero Desktop, use the Shutdown dialog box. To use the thin
  client, you must use your correct password.
- **Use the screensaver** If an administrator has set LockTerminal=2 for the ScreenSaver parameter, and when the screensaver is activated, then the thin client is locked. To unlock the thin client, enter the login password in the unlock dialog box. However, you cannot see the wallpaper while using the unlock dialog box.

# Signing off and shutting down

Use the  ${\bf Shutdown}$  dialog box to select the available option you want:

- · Classic Desktop—Click Shutdown in the Connect Manager or Desktop Menu.
- · Zero Desktop—Click the Shutdown icon on the Zero Toolbar.
- NOTE: You can also configure automatic behavior after all desktop sessions are closed by using the Remote Connections dialog box, see Central configuration: Automating updates and configurations.

# **Battery information**

This section is applicable to the Wyse 5470 Thin Client.

The battery indicator is displayed on the system tray in the classic mode. The battery indicator is displayed on the zero toolbar in the zero mode.

The following table contains the battery indicators:

#### **Table 5. Battery indicators**

Battery status	Icon
While charging with the AC adapter	0
Battery 90% - 100% without connecting the AC adapter	
Battery 50% - 89% without connecting the AC adapter	
Battery 25% - 49% without connecting the AC adapter	
Battery 9% - 24% without connecting the AC adapter	
Battery 0% - 8% without connecting the AC adapter	

- · When the battery is lower than 12%, a notification is displayed at the right-bottom with the remaining percentage.
- Plugging in the AC adapter to charge the device increases brightness by 10% and disconnecting the AC adapter decreases brightness by 10%.
  - NOTE: If you adjust the brightness after disconnecting the AC adapter, the brightness does not change after the adapter is plugged in. In this case, the current brightness replaces the default value.
- · After you plug in or plug out the AC adapter, it takes approximately 5 seconds for the battery icon to be updated.
- By default, the critical battery level is 5%. When the battery reaches the critical level, ThinOS is turned off automatically. You must plug in the AC power to power on the thin client. You can use the INI parameter to change the auto power off settings. For more information about the INI parameters, see the *Dell Wyse ThinOS INI Reference Guide* at www.dell.com/support.

# Sleep mode

The sleep mode enables the power-saving state and quickly resumes full power operations without loss of data.

The sleep mode feature is supported on the following platforms:

- · Wyse 5040 AIO client with ThinOS (5212)
- Wyse 5040 AIO client with PCoIP (5213)
- · Wyse 5070 Thin Client with ThinOS
- Wyse 5070 Thin Client with PCoIP
- Wvse 5470 Thin Client with PColP
- · Wyse 5470 Thin Client with ThinOS
- · Wyse 5470 All-in-One Thin Client PCoIP
- Wyse 5470 All-in-One Thin Client with ThinOS

The USB interface is closed in sleep mode. All USB devices such as USB drives, Bluetooth, audio devices, video devices, and camera are reinitialized after resuming from sleep mode.

The wired network, wireless network, and VPN are disconnected in sleep mode. However, the network configurations are saved.

All the ThinOS configurations—file server, INI, VDI configuration, network configuration, and so on—are saved automatically in sleep mode. The INI parameters are not reloaded from the file server after resuming from sleep mode.

The following windows are not closed in sleep mode:

- · Performance Monitor
- Troubleshooting
- System Information
- System Tools
- · VPN Manager
- · Central Configuration
- · System Preferences
- · Display
- · Printer Set Up
- · Remote Connections

- NOTE: You are logged off from the ThinOS VDI broker and sessions in sleep mode. You must log in to broker sessions again after resuming from sleep mode.
- · Network Set Up
- NOTE: Peripherals windows are closed in sleep mode to reinitialize any peripheral devices after resuming from sleep mode.

## **Enable sleep manually**

To enable the Sleep option manually, use either of the following options:

- ThinOS lock window—To enter sleep mode using the ThinOS lock window, do the following:
  - 1. Lock your thin client.
  - 2. In the ThinOS lock window, click Sleep.
  - Click OK.
- Shutdown dialog box—To enter sleep mode using the Shutdown dialog box, do the following:
  - 1. Open the Connect Manager or the Desktop Menu.
  - 2. Click Sleep, and then click OK.

You can wake the thin client from sleep mode by using the mouse, keyboard, power button, or the Wake-On-LAN feature.

## **Enable automatic sleep**

To enable the thin client to automatically enter sleep mode, do the following:

- 1. From the desktop menu, click System Setup, and then click System Preferences.
- 2. Click the General tab.
  - NOTE: On the Wyse 5470 Thin Client, you must select either Battery or plugged in based on the power supply. If you using the Wyse 5470 All-in-One Thin Client, you can select only plugged in.
- 3. From the Screensaver drop-down list, select the Turn Off Screen option.
- 4. From the After Turn Off screen drop-down list, select the Sleep option.
- 5. From the **Timer** drop-down list, select the idle time after which you need the thin client to enter sleep mode.
  - NOTE: The Screen Saver and After Turn Off Screen options are always the same when the thin client is on battery or if the AC adapter is plugged in. You can change the Timer based on your preference.
- 6. Click OK.

Sleep mode timer starts after screen is turned off by the screensaver. The device automatically enters sleep mode when the ThinOS client is left idle for the specified idle time.

i NOTE: The screen flashes for one second before automatically entering the sleep mode

The thin client takes less than 5 seconds to resume from sleep mode. To resume the thin client from the sleep mode, perform any of the following actions:

- Press the power button.
- · Click the USB mouse or move the wireless USB mouse.
  - (i) NOTE: By default, this feature is disabled. To enable the feature:
    - o On the Wyse 5470 Thin Client, connect the AC adapter to the thin client, and use INI parameter wakeonusb=yes.
    - On the Wyse 5470 All-in-One Thin Client, use INI parameter wakeonusb=yes.
- · Press any key on the USB keyboard.
  - NOTE: By default, this feature is disabled. To enable the feature:
    - o On the Wyse 5470 Thin Client, connect the AC adapter to the thin client, and use INI parameter wakeonusb=yes.
    - $\circ~$  On the Wyse 5470 All-in-One Thin Client, use the INI parameter  ${\tt wakeonusb=yes.}$
- · Press any key on the integrated keyboard. This option is applicable only to the Wyse 5470 Thin Client.
- · Use the Wake on LAN feature to wake up from the sleep mode.
  - i NOTE: On the Wyse 5470 Thin Client, you must connect the AC adapter to the thin client.

On the Wyse 5470 Thin Client, when you resume the system from the sleep mode, the system is first turned off and then turned on to load the ThinOS operating system (cold reboot). This behavior is observed in the following scenarios:

- · If the system has entered the sleep mode for 1 hour.
  - i NOTE: You can change the timer setting using the INI parameter Sleep=yes, MaxSleepPeriod=[0-255].
- · If the Dell Docking Station WD 19 is plugged in or out, and if there is a display attached to the docking station.

# Additional getting started details

This section includes details about zero desktop, classic desktop, login dialog box, and system information.

# Zero desktop features

This section includes information on:

- · Zero interactive desktop guidelines
- Zero toolbar
- · List of connections

## Zero interactive desktop guidelines

The Zero Desktop has a default background with the Zero Toolbar at the left of the screen.

The following network icons are added to the taskbar:

- · Wireless—
- Wired—
- · Default—

The respective icon is displayed based on the connection type and if there is no connection, the default icon is displayed. The network icon is displayed irrespective of whether the Ethernet cable is connected to the thin client. Clicking the network icon displays the **Network Setup** window that can be used to configure your network settings.

The following table lists the available Zero Desktop shortcuts:

#### **Table 6. Zero Desktop shortcuts**

Action	Press
Display the Zero Toolbar	Ctrl+Alt+UpArrow
Open a selection box for toggling between the desktop and currently-active connections	Ctrl+Alt+DownArrow
Lock the thin client	Ctrl+Alt+LeftArrow
	or
	Ctrl+Alt+RightArrow
Keyboard shortcuts to menu commands	Left-Alt+UnderlinedLetter
	or
	Right-Alt+UnderlinedLetter
Capture the full desktop to the clipboard	Print Screen
Capture the active window to the clipboard	Alt+PrintScreen

### (i) NOTE:

- You can copy and paste between application sessions and between sessions and the desktop, however, this function depends on session server configurations.
- In addition to the standard two-button mouse, the thin client supports a Microsoft Wheel Mouse used for scrolling.
   Other similar types of a wheel mouse may or may not work.

To switch the left and right buttons, use the **Peripherals** dialog box, see Configuring the peripherals settings.

#### Zero toolbar

The Zero toolbar usually appears at the left corner of the Zero Desktop. However, depending on administrator configurations, the toolbar can be removed or hidden. It is shown only when a user moves the mouse pointer over the left edge of the desktop screen.

Administrators can configure the toolbar settings using either a dialog box, or the SysMode parameter in the wnos.ini file.

Table 7. Toolbar icons

Icon	What It Does
Home	Opens the list of available connections.
System Information	Displays thin client system information.
System Settings	Opens the System Settings menu to configure thin client system settings and perform diagnostics.
Shutdown Terminal	Click the Shutdown Terminal icon to use the Shutdown options available on the thin client.  i NOTE: The Shutdown Terminal icon does not display on the toolbar when using the Admin Mode button to configure system settings.
Battery indicator	Hover your mouse over the battery indicator to view the remaining battery percentage. This option is applicable only to the Wyse 5470 Thin Client.

NOTE: If configured to display by an administrator, the current date and time are shown on the Zero Toolbar. The thin client is capable of synchronizing its clock to time provided by a Simple Network Time Protocol (SNTP) server.

## List of connections

On the Zero Toolbar, you can click the **Home** icon to open your list of assigned connections. Sometimes, the list contains only default connections.

Use the following guidelines depending on user privilege level, some options may not be available for use:

**Table 8. Connection options** 

Option	What It Does
Name of the connection	Opens the connection you want to use.  i NOTE: All open connections display a blue icon to the left of the connection name in the list.
Reset icon	Resets the connection.  i NOTE: It is useful when a connection is not functioning properly or you need to reboot the connection.
Close icon	Closes the connection.  i NOTE: The Close icon is grayed out for connections that are not open.
Edit icon	Opens the Connection Settings dialog box to change the connection options.  (i) NOTE: Depending on user privilege level, editing options may not be available for use.
Add Connection	Allows you to configure or add new connections.

Table 8. Connection options (continued)

Option	What It Does
Configuring Global Connection Settings	If you do not use INI files to provide global connection settings, you can click <b>Global Connection Settings</b> to open and use the <b>Global Connection Settings</b> dialog box to configure settings that affect all the connection in the list.

# **Using Zero theme**

Use the zero theme option to customize the look and feel of your ThinOS for Citrix, VMware, Classic or VDI mode. To enable a zero theme, deploy the INI parameters based on your zero theme preference, and restart your thin client. The **Visual experience settings are changed** message is displayed, and the thin client loads the selected zero theme.

ZeroTheme={Classic, VDI, Citrix, VMware}

SysMode={Classic, VDI, Citrix, VMware}

INI parameters work with wnos.ini file. You can also use Wyse Management Suite to manage the configuration.

- Citrix zero mode—When you configure ThinOS in Citrix zero mode, the device searches for xen.ini file, and loads the Citrix zero mode. If the xen.ini file is not available, then the wnos.ini file is used during configuration. If you need to switch from the Citrix zero mode, then you must use the wnos.ini file during configuration.
- · VMware zero mode—When you configure ThinOS in VMware zero mode, the device loads the VMware zero mode.
  - NOTE: VMware wallpaper is used in the VMware zero mode.

# Classic desktop features

This section includes information about classic interactive desktop, shortcut menu, desktop menu, and Connect Manager.

# Classic interactive desktop guidelines

The Classic desktop has a Dell Wyse default background with a horizontal task bar at the bottom of the screen.

Use the following guidelines:

- Icons representing available server connections and published applications are displayed on the background. If you pause the mouse
  pointer over an icon, the information about the connection will be displayed. Right-clicking on an icon opens the **Connection Settings**dialog box which displays additional information about the connection. The number of icons that can be displayed on the desktop
  depends on the desktop resolution and administrator configuration.
- A server connection and published application can be opened by double-clicking a desktop icon or a user can navigate to the desktop
  icon they want by using tab key and pressing Enter to initiate the connection.
- · Right-clicking on the desktop provides a shortcut menu, see Using the shortcut menu.
- · Clicking the User Name or clicking on the desktop, opens the desktop menu, see Using the desktop menu.
- A network icon is added to the taskbar on the classic ThinOS desktop. The network icon is displayed irrespective of whether the
  Ethernet cable is connected to the thin client. Clicking the network icon displays the **Network Setup** window that can be used to
  configure your network settings.



Figure 3. Taskbar

### i NOTE:

- · User Name is the user who is logged-on and is located at the lower-left pane of the task bar.
- If configured to display by an administrator, the volume control is displayed in the right corner of the taskbar and the
  current time and date are shown when the cursor is placed on the time; the thin client is capable of synchronizing its
  clock to time provided by a Simple Network Time Protocol (SNTP) server.

## Using the Shortcut menu

To use the Shortcut menu:

- 1. Log in as administrator.
- 2. Right-click on your desktop
  - The Shortcut menu is displayed.
- 3. On the **Shortcut** menu, you are able to view and use the following options:
  - a. Administrator Mode—Allows administrators to configure various settings locally on thin client.
  - b. Hide all windows—Brings the full desktop to the foreground.
  - c. Copy to clipboard—Copies an image of the full screen, current window or event log to the clipboard. The clipboard contents can then be pasted to an ICA or an RDP session. You can copy full screen or current window to clipboard, and can export the screenshots using the Export Screenshot option in Troubleshooting.
  - d. Purge clipboard—Discards the contents of the clipboard in order to free up memory.
  - e. Lock Terminal—Puts the thin client in a locked state if the user has signed on to the system with a password. The thin client can only be unlocked using the same password.
  - f. Group Sessions—Enables you to open more than three ICA, RDP, PCoIP, Blast or ICA seamless sessions. The sessions are displayed as a group on the taskbar.

## Using the desktop menu

To use the desktop menu:

1. Click your desktop or click your User Name.

User Name is the user who is logged-on and is at the lower left side of the taskbar.

The Desktop menu is displayed.

- 2. On the desktop menu, you are able to view and use the following options:
  - a. System Setup Provides access to the following local system setup dialog boxes:
    - **Network Setup** —Allows selection of DHCP or manual entry of network settings, as well as entry of locations of servers essential to thin client operation. This menu selection is disabled for Low-privileged users.
    - Remote Connections—Allows you to configure thin client broker connections including Microsoft, Citrix Xen, Dell vWorkspace, VMware View, Amazon WorkSpaces or Other broker server connections.
    - Central Configuration—Allows you to configure thin client central connection settings such as file server and optional WDA server settings.
    - · VPN Manager Allows you to configure thin client VPN manager.
    - · System Preference—Allows user selection of thin client parameters that are matter of personal preference.
    - · **Display**—Allows you to configure the monitor resolution and refresh rate.
    - Peripherals—Allows you to select the peripherals settings such as audio, keyboard, mouse, serial, camera, bluetooth, and touchscreen settings.
    - · Printer—Allows configuration of network printers and local printers that are connected to the thin client.
  - b. System Information—Provides thin client system information.
  - c. System Tools—Provides information about devices, certificates, packages, global INI, user INI, wdm or ccm.ini.
  - d. **Troubleshooting options**—Displays Performance Monitor graphs that display client CPU, Memory and Networking information, Trace and Event log settings, CMOS management extract and restore settings, and other options that are useful for ThinOS troubleshooting.
  - e. **Applications**—Contains a submenu of all locally configured applications and is populated with published applications when a user is signed on using either PNLite or PNAgent.
  - f. Shutdown—Opens the Sign-off/LockTerminal/Shutdown/Restart the System dialog box.

## Using the Connection Manager

To use the Connection Manager:

- 1. Click Connect Manager on the taskbar.
  - · The Connect Manager has a list of connection entries and a set of command buttons available for use with the connections.
  - · Non-privileged users cannot view the Connect Manager.

The Connection Manager dialog box is displayed.

- 2. In the Connection Manager dialog box, use the following buttons to configure the Connection Manager settings:
  - a. Click Connect to select a connection from the list and make a connection.
  - b. Click **New** to open the **Connection Settings** dialog box either directly or through the Connection Protocol menu selection for creating a new connection definition.

The locally defined connections are added to the connection list. Be aware of the following information:

- High-privileged user—Typically, all locally defined connection definitions are temporary and are lost when the user logs off
  and when the thin client restarts or is shut down. However, if configured by an administrator (enablelocal=yes), locally defined
  connection definitions can be saved in these cases.
- Stand-alone user—Locally defined connections are retained when the thin client restarts or is shut down and there is no individual logon. Network configuration settings must be made locally.
- c. Click Properties to open the Connection Settings dialog box for the selected connection.

Be aware of the following information:

- High-privileged user—Can view and edit the definitions for the currently selected connection. Edits are not permanently retained when the user signs-off.
- Low-privileged user—Cannot create or edit connections, but can view connection definitions. However, you can enable a low-privileged user to create a connection using INI parameters.
- · Stand-alone user—Can permanently modify the persistent connections except when PNAgent/PNLite services are used.
- d. Click Sign-off to sign off from the thin client.
- e. Select a connection from the list, and click delete to delete the selected connection.
- f. Select a Virtual connection from the list, and click Reset VM to reset a selected virtual connection.
- g. Click Global Connection Settings tab to open and use the Global Connection Settings dialog box to configure settings that affect all the connections in the list.

# Login dialog box features

While the **Login** dialog box allows you to log on to the server, it also allows you to:

- · Obtain system information.
- Access Admin Mode to configure thin client settings.
- · Change or reset your own password, and unlock your account.
- Open the **Shutdown** dialog box by using CTRL+ALT+DELETE.

In the **Login** dialog box, use the following guidelines:

- System Information—Click the Sys Info button to open the System Information dialog box. You can view the thin client system information such as System Version, IP Address, information on devices connected to your thin client, event logs and so on.
- Admin Mode—Click the Admin Mode button to configure various settings locally on the thin client other than broker desktop configurations. For example, you can choose to manually configure the Citrix XenBroker Server URL or override the URL that is centrally defined by file servers by using the Remote Connections dialog box as described in Remote Connections.
  - o Classic desktop—Use the Leave Administrator Mode option in the Shutdown dialog box.
  - Zero desktop—Use the Leave Administrator Mode option in the Shutdown dialog box, or use the Leave Administrator Mode icon (X) in the upper-right pane of the System Settings menu.
  - NOTE: By default the Admin Mode button is not displayed on the log on dialog box. You can display it by selecting the Show local admin button check box in the Shutdown dialog box.
  - NOTE: By default there is no password needed for the Admin Mode button use. You can password protect the Admin Mode button (to require login credentials) by using the AdminMode parameter in a wnos.ini file, see Dell Wyse ThinOS INI Guide.
- **Shutdown**—Click the **Shutdown** button to open and use the **Shutdown** dialog box to sign off, shut down, restart, reset the system setting to factory defaults, and so on.
- Account Self-Service—Click the Account Self-Service icon shown when configured using the AccountSelfServiceoption of
  the PasswordServer INI parameter to open and use the Account Self-Service dialog box to change or reset your own password
  and unlock your account. For information on INI parameter, see Dell Wyse ThinOS INI Guide.

This process assumes that the security questions and answers have been pre-registered by the user inside their Windows environment. Users must use HTTPS (not HTTP) for an account self-service server address such as Https://IPAddress, in the **Broker Setup** tab. After the security questions are answered, your new password will be set or your account will be unlocked.

# Word wrap feature

The word wrap feature enables you to fit large text inside the available display area of the active window.

To enable the word wrap feature, use the INI parameter wordwrap.

For example, noticefile=dell notice resizable=no wordwrap=yes.

The default value is no. When you change the value to yes, the text is confined to the display area and the horizontal scroll bar is disabled.

# **Accessing system information**

Use the **System Information** dialog box to view system information.

- · Classic desktop—Click System Information from the desktop menu.
- · Zero desktop—Click the System Information icon on the zero toolbar.

The **System Information** dialog box includes:

- General tab—Displays general information such as System Version, Serial Number, Memory Size (Total and Free), CPU Speed, ROM Size, Monitor, Parallel ports, Terminal Name, Boot from, Memory speed, SSD size, Resolution, and the Serial ports.
- · Copyright tab—Displays the software copyright and patent notices.

Acknowledgments button is added in the Copyright tab in System Information. This button is related to third party software.

Event Log tab—Displays the thin client start-up steps normally beginning from system version to checking firmware or error messages that are helpful for debugging problems. The details about the monitors and USB connected to the thin client, and bluetooth initialization are also displayed.

When you install packages or restart the ThinOS device, the ThinOS client verifies the version of the installed package. If you have not installed the latest package version, the details about the current package version and the recommended package version are displayed.

Status tab—Displays status information about TCP performance related parameters, UDP performance related parameters, CPU Busy, System Up Time, Wyse Management Suite status, Free Memory, Active sessions, and WDM status.

On the Wyse 5470 Thin Client, the battery percentage and the estimated battery time remaining are displayed. When the AC adapter is plugged in and charging, the remaining time is displayed as Charging.

- · IPv6 tab—Displays IPv6 information such as Link-local Address, IPv6 Address, and IPv6 Default Gateway.
  - NOTE: This tab is displayed when IPv6 is enabled in the General tab of the Network Setup dialog box.
- **ENET tab**—Displays information about wired network connections.
- · WLAN tab—Displays information about wireless network connections.
- · About tab—Displays information about the ThinOS operating system. The following attributes are listed:
  - Platform name
  - Operating system type
  - ThinOS build name
  - ThinOS build version
  - o BIOS name
  - o BIOS version
  - o Citrix Broker or Receiver version—This represents ICA revisions between the ThinOS versions.
  - Dell vWorkspace version
  - o VMware Horizon version—This represents the Horizon revisions between the ThinOS versions.
  - o Microsoft Broker or RDP version
  - Teradici PCoIP version—This represents the PCoIP revisions between the ThinOS versions, and is applicable to the PCoIP devices only.
  - Imprivata version
  - Caradigm version
  - SECUREMATRIX version
  - HealthCast version



- Kernel mode—The components are implemented in Kernel according to the specification. The version is displayed as [max].[min], which is the base version of protocol or server or client of the component. For example, the Microsoft RDP protocol version is 10.0, the Imprivata version is 5.2, and so on.
- User mode—The components are from the source, or binaries from third party that are 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 component, and the [svn\_revision] is the source control revision of ThinOS. Using the ThinOS specified version, you can identify the changes between different revisions. For example, the Citrix Receiver version is 14.0.44705, the VMware Horizon version is 4.8.x, and so on. The components are matched to the installed packages. If the packages are removed, the field remains empty in the About tab.

# **ENERGY STAR compliance**

ENERGY STAR is a standard label on devices that meet energy-efficiency requirements by Environmental Protection Agency (EPA). Wyse 5070, Wyse 5470, and Wyse 5470 All-in-One thin clients with ThinOS are ENERGY STAR compliant. For more information about the ENERGY STAR program, see <a href="https://www.energystar.gov">www.energystar.gov</a>.

ThinOS-based devices are ENERGY STAR 8 compliant. To enable or disable ENERGY STAR 8 on your thin client, deploy the INI parameter enableEEE={0,1}.

### IPv6 certification

All networks are required to be Internet Protocol version 6 (IPv6) capable. Wyse 5070, Wyse 5470, and Wyse 5470 All-in-One thin clients with ThinOS are certified for IPv6 capability.

# **Global Connection settings**

Use the Global Connection Settings dialog box to configure the connection settings such as ICA, RDP, Horizon, and PCoIP.

- · Zero desktop—Click **Global Connection Settings** in the list of connections.
- · Classic desktop—Click Global Connection Settings in Connect Manager.

To configure the Global Connection settings:

- On the desktop taskbar, click Connect Manager > Global Connection Settings.
  The Global Connection Settings dialog box is displayed.
- 2. Click the **Session** tab to configure the options that are available to all sessions.

The Smart Card check box specifies the default setting for connecting to a smart card reader at system startup.

(i) NOTE:

ICA sessions automatically connect when you connect the smart card readers. If you want to use the Disks option to automatically connect to ICA sessions, use the following guidelines:

- More than one disk can be used simultaneously. However, the maximum number of USB drives including different subareas is 12.
- Ensure that you save all data and sign off from the session before removing the USB drive.
- NOTE: USB devices redirection—By default, audio, video, and printer devices do not use HDX USB for redirection.
  You can make selections for USB device redirection on the Session tab of the Global Connection Settings dialog box.
- 3. Click the ICA tab, and do the following:
  - a. Select the check boxes for the options that are available to all ICA sessions.
  - **b.** Select an audio quality optimized for your connection.
  - c. Use the Map to option to map a disk. When a drive is entered, the disk is mapped in the corresponding drive.
- 4. Click the RDP tab, and do the following:
  - a. Select the Enable Network Level Authentication (NLA) check box if you want to verify users before connecting to a full RDP connection.
  - b. Select the **ForceSpan** check box to span the session horizontally across two monitors. This option enables you to use two monitors as one large monitor.
  - c. Select the **Enable TSMM** check box if you want to enable the Terminal Service Multimedia Redirection.
  - d. Select the Record From Local check box if you want to enable recording from a local microphone.
  - e. Select the **RemoteFX** check box to enable RemoteFX. RemoteFX is used to remotely deliver Windows virtual desktops over a network connection.
  - **f.** From the **USB Redirection Type**, select RDP USB. To use RDP USB, you must use a RemoteFX session for Windows 7/Windows 2008 R2 session. However, RDP USB is not supported using a standard Windows 7/Windows 2008 R2 session. For Windows 8 session and later, RDP USB is supported.
  - g. In the **Desktop Scale Factor** box, enter the DPI value in percentage. This option enables you to define the desktop DPI remotely. The Desktop Scale Factor is only applicable for the RDP connection. Setting this option does not impact the display scale of the thin client locally. The DPI range is 100–500. If you enter a nonnumeric character, the value is automatically set to 100. If you enter a value less than 100, the value is automatically set to 500.
    - NOTE: The desktop scale factor is applicable only to RDP version 8, and RDP 10 or higher versions. RDP version 7 is not supported.
- 5. Click the Horizon tab, and do the following:
  - a. Select the Enable H264 check box. This option enables the H.264 decoding in Horizon Client. Enabling this option, improves the performance of high-end applications. H.264 is disabled by default. To validate the H.264 decoding, add an INI parameter setenv BlastDebugClientH264=yes, and verify if the H264 basic watermark is displayed in the upper-left corner of the VMware Blast session window.



- Blast H.264 feature is not supported on Wyse 5010 thin clients, Wyse 5040 thin clients, and Wyse 7010 thin clients. Blast H.264 is automatically disabled on Wyse 5060 thin client for 1920 x 1200 resolution due to hardware limitation.
- A performance tracker is introduced by VMware for performance evaluation and data collection.
- b. From the Network Condition drop-down list, select whether to use a condition for your Blast connection.
  - NOTE: Blast Extreme protocol is part of Blast Extreme Advanced Transport (BEAT).
  - · Select **Excellent** to enable the Blast connection to use Transmission Control Protocol (TCP).
  - · Select Typical to enable the Blast connection to use Transmission Control Protocol (TCP). By default, this value is selected.
  - Select **Poor** to enable the Blast connection to use User Datagram Protocol (UDP). UDP uses the available bandwidth to deliver the user experience.

To enable UDP, you must modify the VMware View Connection Server, the Agent host desktop, and the VMware Horizon Client settings. For information about the necessary configuration on server and agent desktop, see the VMware Certificate Guide at code.vmware.com/group/euc/thin-client/certs/4.6.

c. Select the **High Color Accuracy** check box. This option enables Horizon Client to use a superior color fidelity when H.264 decoding is enabled.

The **High Color Accuracy** option is available on the following platforms:

- Wyse 3030 LT thin client
- · Wyse 3040 thin client
- · Wyse 5060 thin client
- · Wyse 5070 thin client

In PCoIP-enabled clients, the **PCoIP** tab is available. Select the **USB device redirection** type from the drop-down list. The available values is **PCoIP USB**.

# **Configuring connectivity**

This chapter helps you to understand various configuration settings for a secure connection.

To configure the settings on Classic desktop, click **System Setup** from the desktop menu, and use the configuration tabs. To configure the settings on Zero desktop, click the **System Settings** icon on the zero toolbar, and then use the configuration tabs.

# Configuring the network settings

Use the network options to configure the network based on your requirement.

## Configuring the general settings

To configure the general network settings:

- From the desktop menu, click System Setup, and then click Network Setup. The Network Setup dialog box is displayed.
- 2. Click the **General** tab, and use the following guidelines:
  - a. Select the network interface options based on your thin client model.
    - To set the default gateway on supported ThinOS platforms with Wireless LAN (WLAN) module, select the type of network interface from the following options:
      - ENET— Enables you to set up the Ethernet Wired Network connection using the onboard Ethernet port.
      - WLAN—Enabled you to set up a Wireless Network connection.

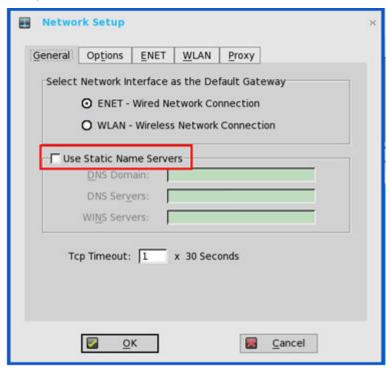


Figure 4. General settings with ENET and WLAN

- To set the default gateway on Wyse 5070 thin client contains any of the optional modules—Registered Jack 45 (RJ45) or Small form-factor pluggable (SFP) module, select the type of network interface from the following options:
  - ENETO— Enables you to set up the first Ethernet Wired Network connection using the onboard Ethernet port.
  - ENET1—Enables you to set up the second Ethernet Wired Network connection using the Ethernet port on the docking station.

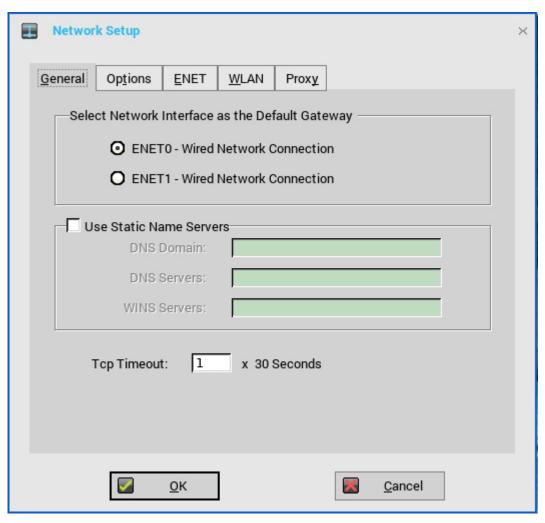


Figure 5. General settings with ENET0 and ENET1

- To set the default gateway on the Wyse 5470 Thin Client with the Dell Docking Station WD19, select the type of network interface from the following options:
  - ENETO— Enables you to set up the first Ethernet Wired Network connection using the onboard Ethernet port.
  - ENET1—Enables you to set up the second Ethernet Wired Network connection using the Ethernet port on the docking station.
  - **WLAN**—Enables you to set up a Wireless Network connection.

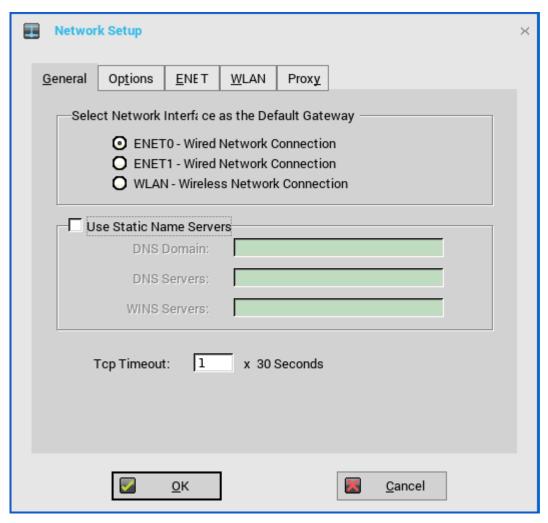


Figure 6. General settings with ENET0, ENET1, and WLAN

ThinOS supports the following network combinations on the Wyse 5470 Thin Client:

- Onboard Ethernet port + Ethernet port on the docking station
- · Onboard Ethernet port + Wireless
- Ethernet port on the docking station + Wireless
  - (i) NOTE: You do not need to reboot the system when you connect or disconnect the Dell WD 19 docking station for the network to work.

You can connect your thin client to two wired network connections at the same time. The default gateway is determined by the user interface settings. However, user interface is not changed automatically.

**Onboard Ethernet port + Ethernet port on the docking station + Wireless**—You can use the combination of these three network interfaces together. However, the following are the known issues while using this combination:

- You can connect to the network using any two network interfaces and select the network interface that is not connected as
  default. The network can be used in this scenario, but the preferred network type cannot be determined.
  - For example, you can connect to the network using the two Ethernet ports and select the **WLAN** option on the user interface as default without connecting to a wireless network. The network can be used in this scenario, but the preferred network type cannot be determined.
- You can connect to the network using all three available network interfaces together. The preferred network type cannot be determined in this scenario.
- b. **Use Static Name Servers**—By default, this check box is not selected, and thin client fetches the server IP address from DHCP. Select this check box to manually assign static IP addresses.

If name servers are changed using GUI, INI or link down/up, then the details are displayed in Event Logs.

In dynamic mode, the DNS/WINS can be merged from Ethernet 0 and Ethernet 1, if network is not working.

i. Enter the URL address of the DNS Domain in the DNS Domain box.

ii. Enter the IP address of the DNS Server in the DNS Server box.

Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. Enter the DNS Domain and the network address of an available DNS Server. The function of the DNS Domain entry is to provide a default suffix to be used in name resolution. The values for these two boxes may be supplied by a DHCP server. If the DHCP server supplies these values, they replace any locally configured values. If the DHCP server does not supply these values, the locally configured values will be used.

- NOTE: You can enter up to 16 DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server and the rest are secondary DNS servers or backup DNS servers.
- iii. Enter the IP address of the WINS Server in the WINS Server box.

Use of WINS is optional. Enter the network address of an available WINS name server. WINS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. These entries can be supplied through DHCP, if DHCP is used. DNS and WINS provide essentially the same function, name resolution. If both DNS and WINS are available, the thin client attempts to resolve the name using DNS first and then WINS.

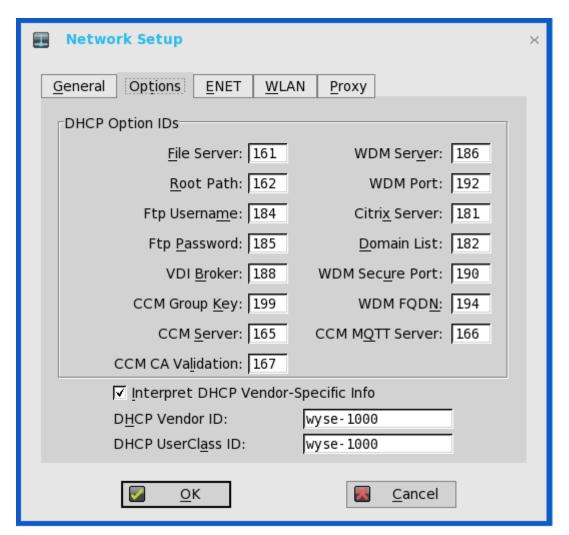
You can enter two WINS Server addresses (primary and secondary), separated by a semicolon, comma, or space.

- c. Enter the digit multiplier of 30 seconds in the **TCP Timeout** box to set the time-out value of a TCP connection. The value must be **1** or **2** which means the connection time-out value is from 1x30= 30 seconds to 2x30= 60 seconds. If the data for connecting to the server is not acknowledged and the connection is time out, setting the time-out period retransmits the sent data and again tries to connect to the server till the connection is established.
- 3. Click **OK** to save the settings.

### Configuring the DHCP options settings

To configure the options settings:

- From the desktop menu, click System Setup, and then click Network Setup. The Network Setup dialog box is displayed.
- 2. Click the **Options** tab, and use the following guidelines:



- a. **DHCP Option IDs** Enter the supported DHCP options. Each value can only be used once and must be between **128** and **254**. For information about DHCP options, see DHCP options.
- b. Interpret DHCP Vendor-Specific Info Select this check box for automatic interpretation of the vendor information.
- c. DHCP Vendor ID Shows the DHCP Vendor ID when the dynamically allocated over DHCP/BOOTP option is selected.
- d. DHCP UserClass ID Shows the DHCP UserClass ID when the dynamically allocated over DHCP/BOOTP option is selected.
- 3. Click **OK** to save the settings.

### Configuring the ENET settings

To configure the ENET settings:

- From the desktop menu, click System Setup, and then click Network Setup. The Network Setup dialog box is displayed.
- 2. Click the **ENET** tab, and use the following guidelines:

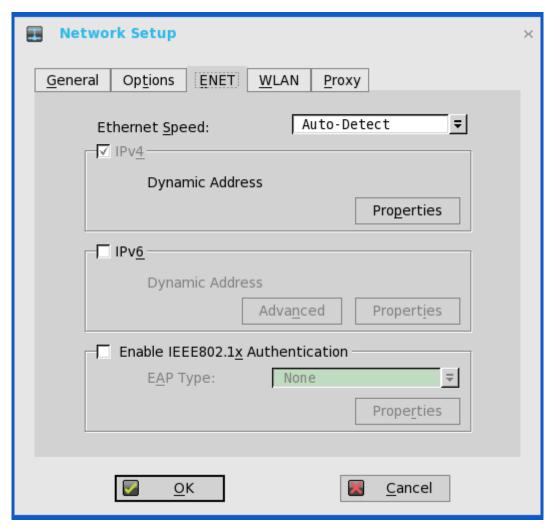


Figure 7. ENET tab

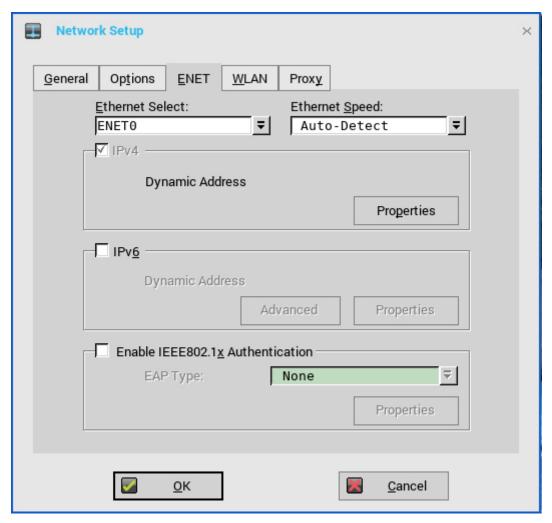


Figure 8. ENET tab

- a. Ethernet Select—Allows you to select the wired network connection. For Wyse 5070 thin client without SFP or RJ-45 module, the ENETO option is selected by default. For Wyse 5070 thin client with SFP or RJ-45 module, select either ENETO or ENET1 based on your network preference.
- b. Ethernet Speed—The default value is Auto-Detect. If your network equipment does not support the automatic negotiation, select any of the available options—10 MB Half-Duplex, 10 MB Full-Duplex, 100 MB Half-Duplex, 100 MB Full-Duplex, or 1 GB Full-Duplex.
  - The 10 MB Full-Duplex option can be selected locally. However, this mode can be negotiated through Auto-Detect.
- c. The IPv4 check box is selected by default. Click Properties to configure the following options:
  - **Dynamically allocated over DHCP/BOOTP**—Select this option to enable your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server by using DHCP options to provide information. Any value that is entered locally in the **Options** tab is replaced by the DHCP value. If the DHCP server fails to provide replacement values, the locally entered value is used.
  - · Statically specified IP Address—Select this option to manually enter the IP address, subnet mask, and default gateway.
    - IP Address—Enter a valid network address in the server environment. The network administrator must provide this information.
    - Subnet Mask—Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices—same subnet or other subnet. If the location is a different subnet, messages that are sent to that address must be sent through the default gateway. This does not depend on the value that is specified through local configuration or through DHCP. The network administrator must provide this value.
    - Default gateway—Use of gateways is optional. Gateways are used to interconnect multiple networks—routing or delivering IP packets between them. The default gateway is used for accessing the Internet or an Intranet with multiple subnets. If no gateway is specified, the thin client can only address other systems on the same subnet. Enter the address

of the router that connects the thin client to the Internet. The address must exist on the same subnet as the thin client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.

d. Select the IPv6 check box, and then click Advanced to select various IPv6 supported setting options from the available check boxes.

The following check boxes are displayed in the IPv6 Advanced Settings dialog box:

- Allow IPv4 to be disabled when IPv6 is enabled
- · Prefer IPv4 over IPv6 when both are available
- Disable Stateless Address autoconfiguration (SLAAC)
- · Disable Duplicate Address Detection (DAD)
- · Disable ICMPv6 Echo Reply
- · Disable ICMPv6 Redirect Support
- · Use Standard DHCPv6 timers

Click **Properties**, and use the following guidelines:

- Wait DHCP—Select this option to enable your thin client to consider IPv6 DHCP before you log in. If you do not select this
  option, and DHCP is enabled, the system still waits for IPv4 DHCP.
- **Dynamically allocated over DHCP/BOOTP**—Select this option to enable your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server (using DHCP options) to provide information. Any value that is entered locally in the **Options** tab is replaced by the DHCP value. If the DHCP server fails to provide replacement values, the locally entered value is used.
- · Statically specified IP Address—Select this option to manually enter the IP address, subnet mask, and default gateway.
  - IP Address—Enter a valid network address in the server environment. The network administrator must provide this information.
  - Subnet Prefix Len—Enter the prefix length of the IPv6 subnet.
  - o Default gateway—Use of gateways is optional. For more information, see various IPv4-supported options in this section.
- **DNS servers**—Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS is used to make the connection. Enter the network address of an available DNS server. The value for this box may be supplied by a DHCP server. If the DHCP server provides this value, it replaces any locally configured value. If the DHCP server does not provide this value, the locally configured value is used.
- NOTE: If you enable IPv6 for both ENET0 and ENET1, IPv6 routes through the Ethernet connection that fetches the IPv6 address first.
- e. Select the Enable the IEEE802.1x authentication check box, and from the EAP type drop-down list, select TLS, LEAP, PEAP
  or FAST.
  - · TLS—Select this option, and click Properties to configure the Authentication Properties dialog box.
    - o Select the Validate Server Certificate check box because it is mandatory to validate your server certificate.
      - NOTE: The CA certificate must be installed on the thin client. The server certificate text field supports a maximum of approximately 255 characters, and supports multiple server names.
    - Select the **Connect to these servers** check box, and enter the IP address of server.
    - o Click Browse to find and select the client certificate file and the private key file you want.
      - NOTE: Ensure that you select the PFX file only.
    - From the Authenticate drop-down list, select either user authentication or machine authentication that is based on your choice.

The following kinds of server names are supported—all examples are based on Cert Common name company.dell.com:

- \*.dell.com
- \*dell.com
- \*.com
- NOTE: Using only the FQDN, that is, company.dell.com does not work. Use one of the options, for example servername.dell.com (\*.dell.com is the most common option as multiple authentication servers may exist).
- **LEAP**—Select this option, and click **Properties** to configure the **Authentication Properties** dialog box. Be sure to use the correct username and password for authentication. The maximum length for the username or the password is 31 characters.

- PEAP—Select this option, and click Properties to configure the Authentication Properties dialog box. Be sure to select either EAP\_GTC or EAP\_MSCHAPv2, and then use the correct username, password, and domain. Validate Server Certificate is optional.
- FAST—Select this option, and click Properties to configure the Authentication Properties dialog box. Be sure to select either EAP\_GTC or EAP\_MSCHAPv2, and then use the correct username, password, and domain. Validate Server Certificate is optional.

To configure EAP-GTC, enter the username only. The password or PIN is required during the authentication process. To configure EAP-MSCHAPv2, enter the username, password, and domain.

i NOTE: The domain\username in the username box is supported, but you must leave the domain box blank.

The CA certificate must be installed on the thin client, and the server certificate validated forcibly. When EAP-MSCCHAPV2 is selected for PEAP or FAST authentication, an option to hide the domain is available. Username and Password boxes are available for use, but the **domain** text box is disabled.

When EAP-MSCHAPV2 is selected for PEAP or FAST authentication, a check box to enable the Single Sign-On feature is available.

From ThinOS 8.3, EAP-FAST authentication is supported. During the initial connection, when there is a request for a Tunnel PAC from the authenticator, the PAC is used to complete the authentication. The first-time connection always fails, and the subsequent connections succeed. Only automatic PAC provisioning is supported. The user/machine PAC provisioning that is generated with CISCO EAP-FAST utility is not supported.

- 3. Click **OK** to save the settings.
  - NOTE: From ThinOS version 8.5, client reboot is not required to change the network settings. All the changes take effect immediately.

For example, ThinOS connects to the new wireless SSID immediately without reboot.

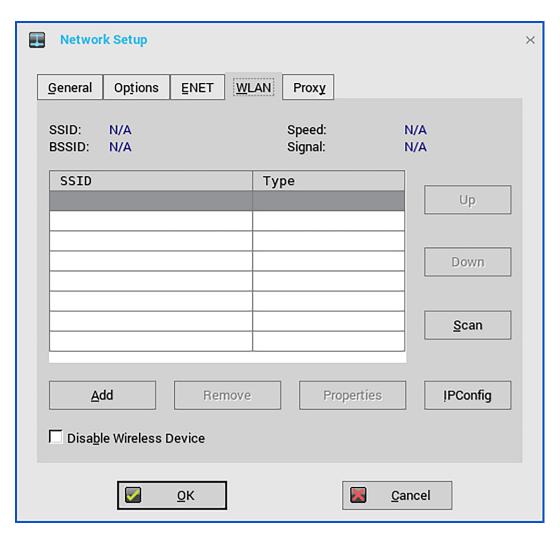
## Configuring the WLAN settings

NOTE: On Wyse 5070 thin client with an optional SFP module or RJ45 module, you cannot configure the wireless settings.

To configure the WLAN settings:

1. From the desktop menu, click **System Setup**, and then click **Network Setup**.

The **Network Setup** dialog box is displayed.



- 2. Click the WLAN tab, and do the following:
  - a. Add—Use this option to add and configure a new SSID connection.

You can configure the SSID connection from the available security type options.

After you configure the SSID connection, the added SSID connection is listed on the WLAN tab.

- **b. Remove**—Use this option if you want to remove an SSID connection from the list.
- c. **Properties**—Use this option to view and configure the authentication properties of an SSID connection that is displayed in the list.
- **d.** Select the **Disable Wireless Device** check box if you want to disable a wireless device.
  - · Always—Click this radio button if you want to disable the wireless device always.
  - EnetUp—Click this radio button if you want to disable the wireless device whenever the wired network is connected.
- e. Click **IPConfig** to configure the IPv4 settings for the wireless connection. To use either DHCP or static IP address, do the following:
  - i. Click Properties.

The **Network Setup** dialog box is displayed.

- ii. To set the IPv4 connection, configure any one of the following options:
  - If you want to allow your thin client to automatically receive information from the DHCP server, click **Dynamically allocated over DHCP/BOOTP**.
  - · If you want to manually configure the IP address, click Statically specified IP Address, and provide the IPv4 details.
- 3. Click **OK** to save the settings.
  - NOTE: Device reboot is not required to change the network settings. All the changes take effect immediately.

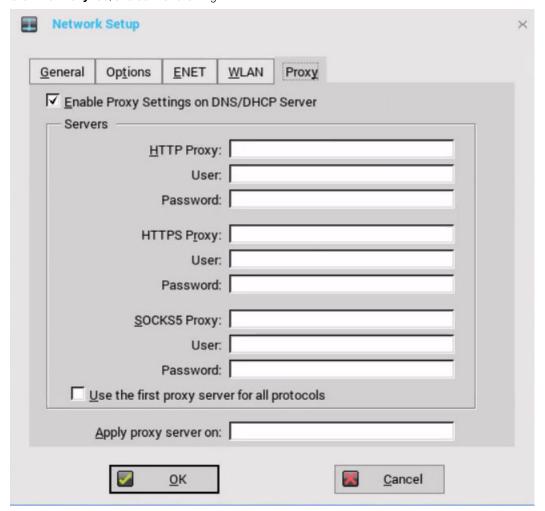
For example, ThinOS connects to the new wireless SSID immediately without reboot. However for ARM platforms—Wyse 3010 thin client, and Wyse 3020 thin client—requires reboot.

### Configuring the proxy settings

The network **Proxy** tab supports Wyse Management Suite, HDX Flash Redirection, and RealTime Multimedia Engine (RTME).

Supported protocols—HDX FR, WMS and RTME

- · For HDX FR: HTTP and HTTPS protocols are supported.
  - o If both HTTP and HTTPS are configured, the HDX FR works with HTTPS proxy.
  - User credential pass through is possible with \$UN/\$PW.
- For Wyse Management Suite: HTTP, HTTPS and Socks5 (recommended) protocols are supported.
- · For **RTME**: HTTP, and HTTPS protocols are supported.
- From the desktop menu, click System Setup, and then click Network Setup. The Network Setup dialog box is displayed.
- 2. Click the **Proxy** tab, and do the following:



- a. Select the Enable Proxy Settings on DNS/DHCP Server check box to use DHCP option tags or DNS records for defining the Wyse Management Suite proxy (SOCKS5) information. By default, this option is selected. You can fetch proxy settings using the DHCP option or DNS SRV records during the system bootup. The DNS record takes precedence over the DHCP option tag. There are two ways to enable or disable this option—ThinOS GUI and INI parameter.
- b. Enter the HTTP proxy port number or HTTPS proxy port number, User name and Password in the respective fields. However, credential pass through (\$UN/\$PW) is not recommended because it starts before user sign on.

Wyse Management Suite uses both HTTP/HTTPS and MQTT protocols to communicate with the WMS/MQTT server. However, the HTTP proxy cannot redirect TCP packages to the MQTT server which requires a SOCKS5 proxy server. If there is only HTTP server available, then the real-time command that requires MQTT does not work.

- HTTP/HTTPS proxy default port is 808, and SOCKS5 proxy default port is 1080.
- c. Select the Use the first proxy server for all protocols check box to allow all the protocols to use the same server in the HTTP Proxy fields. Both HTTP and HTTPS proxy use the same host and port, and SOCKS5 proxy agent uses HTTP host with default Socks5 port (1080).
  - If **SOCKS5 proxy** is configured, then WMS proxy uses the SOCKS5 only. If SOCKS5 is not configured, then WMS proxy searches for alternative protocols, for example, HTTP in the configuration.
- d. Specify the supported applications as Wyse Management Suite, FR and RTME separated by a semicolon in the Apply proxy server on field.
- 3. Click **OK** to save the settings.

#### User scenario

- 1. Configure correct proxy server host and port.
- 2. Configure the user credentials according to the proxy server settings.
  - On system restart, the client checks in to the Wyse Management Suite server through SOCKS5 proxy server. MQTT connection is established through SOCKS5 proxy server. Real-time commands work fine through SOCKS5 proxy server.
- 3. Connect to the Citrix desktop, configure proxy in internet options of the browser, and then playback HDX FR through the HTTP/ HTTPS proxy authentication.

# Configuring the remote connections

Use the **Remote Connections** dialog box to configure thin client remote connections including ICA, RDP, Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop), Microsoft, VMware View, Dell vWorkspace, and other Broker agent server connections. This dialog box also enables you to configure visual options, and general connection settings.

NOTE: In the Classic Desktop option, the Remote Connections dialog box allows you to create the default RDP connections for use. If you want to create more than the default connections, use the Connect Manager. For more information, see Using the Connect Manager.

### Configuring the broker setup

To configure the broker setup:

- From the desktop menu, click System Setup, and then click Remote Connections.
  The Remote Connections dialog box is displayed.
- 2. In the Broker Setup tab, from the drop-down list, select the Broker type.
  - a. Select None, and click either of the following connection protocols:
    - ICA—For more information, see Configuring ICA connections.
    - RDP—For more information, see Configuring RDP connections.
  - b. Select any one of the available broker connections, and configure the broker setup to connect to the respective virtual desktop environments. For instructions about configuring a particular broker setup, see Configuring the connection brokers.

The available broker connections that you can configure on ThinOS are:

- Citrix Xen
- VMware View
- Microsoft
- Dell vWorkspace
- Amazon vWorkspace—This is applicable only to the PCoIP clients.
- · Teradici Cloud Access
- c. Select Other, and use the following guidelines:
  - Broker Server—Enter the IP address of the Broker server.
  - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be listed. Each desktop name is separated by a semi-colon, and is case-sensitive.
- 3. Click **OK** to save the settings.

### Multiple logins with Citrix and VMware Horizon

ThinOS supports PNA multiple login feature. You can log in to multiple Citrix StoreFront or PNAgent using different credentials. From this release onwards, you can simultaneously log in to Citrix StoreFront/PNAgent and the VDM server.

To configure the multiple login feature, do the following:

1. Configure the Pnlite server and VDI broker in the INI file as follows:

```
SelectServerList=vdm; \
description="description" host=<fqdn of Horizon Server>
SelectServerList=pna; \
description="description" host=<fqdn of StoreFront Server>
```

Or

```
multilogon=yes
pnliteserver=<fqdn of StoreFront Server>
VDIBroker=<fqdn of Horizon Server>
```

Or

```
multilogon=yes
SelectServerList=vdm; \
description="description" host=<fqdn of Horizon Server>
SelectServerList=pna; \
description="description" host=<fqdn of StoreFront Server>
```

2. In the login window, select either the Citrix or VMware broker to log in, or log in to both Citrix and VMware brokers with different credentials.

#### Limitation

ThinOS supports a single VDM login even if the MultiLogon parameter is set to yes. When you log in to the first VDI broker successfully, the succeeding VDI brokers are ignored.

For example:

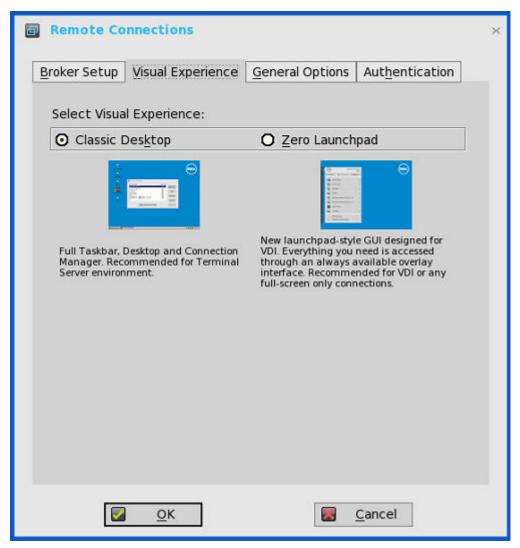
```
multilogon=yes
VDIBroker=<fqdn of Horizon Server 1>;
VDIBroker=<fqdn of Horizon Server 2>
```

If the first VDI broker login is successful, the second VDI broker is ignored. If the first VDI broker login fails, the second VDI broker is considered.

# Configuring the visual settings

To configure the visual settings:

- From the desktop menu, click System Setup, and then click Remote Connections.
   The Remote Connections tab is displayed.
- 2. Click Visual Experience tab, and use the following guidelines:



- NOTE: The Visual Experience tab is grayed out, if the StoreFront Style check box is selected for a Citrix Broker Server entered in the Broker Setup tab.
- a. Classic Desktop Displays the full taskbar, desktop and Connect Manager familiar to ThinOS users. This option is recommended for terminal server environments and for backward compatibility with ThinOS 6.x versions.
- b. **Zero Launchpad** Displays the new launch pad style GUI designed for VDI use. Functionality is accessed through an always available interface. This option is recommended for VDI and any full-screen only connections. Toolbar, hotkey and connection icon options are also available for configuration.

If you select the **Zero Launchpad**, then use the following guidelines:

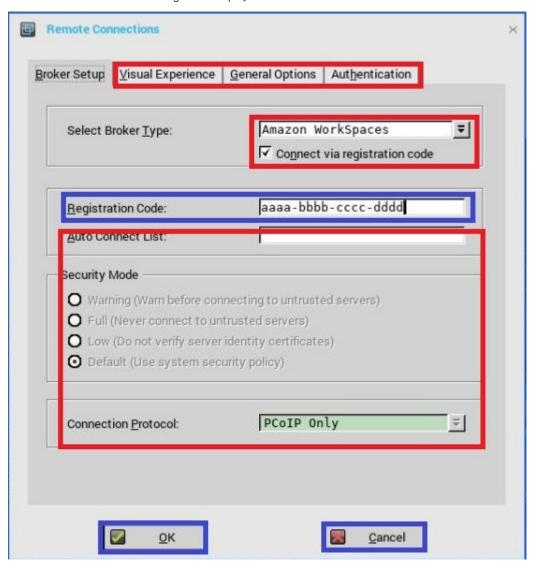
- · Select the check box to enable Zero Toolbar activation in left pane.
  - Select the button if you want to enable Zero Toolbar activation in left pane when you pause a mouse on the screen. You
    must select the time duration—0. 0.5 or 1 second—after which the Zero toolbar is activated.
  - o Select the button if you want to enable Zero Toolbar activation in left pane only after clicking.
- · Select the check box to disable hotkey to show toolbar.
- · Select the check box to always disable toolbar when you have one session available.
- · Select the check box to disable the Home icon.
- 3. Click **OK** to save the settings.

## Configuring the general options

To configure the general options:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The Remote Connections dialog box is displayed.



- 2. Click the **General Options** tab, and use the following guidelines:
  - a. Click the available options to select the action after you exit all open desktops. The available options are **None**, **Sign-off** automatically, **Shut down the system automatically** and **Restart the system automatically**.
    - i NOTE: By default, None is selected and the thin client automatically returns to the terminal desktop.
  - b. **Default Sign-on Username** Enter the Default user name.
  - c. Default Sign-on password— Enter the Default password.
  - d. **Default Sign-on Domain** Enter the Default Domain.
  - e. Click Clear locally saved connections to clear locally saved connections.
    - NOTE: If you enter all three default sign-on credentials (Username, Password and Domain), you are automatically logged on to your desktop upon system start.

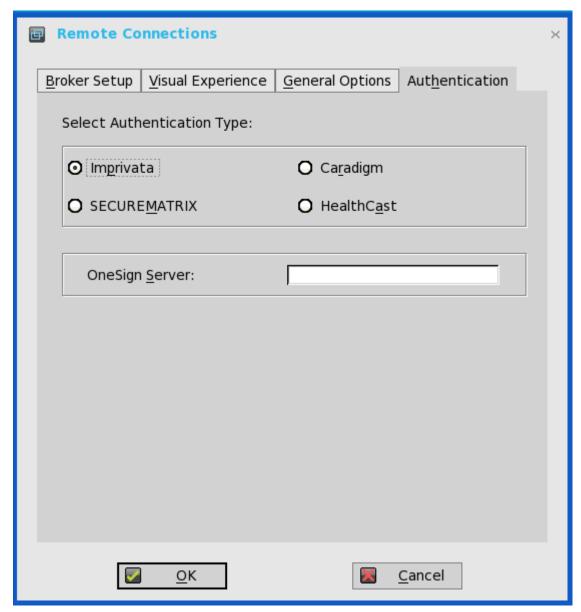
### Configuring the authentication settings

To configure the authentication settings:

- 1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
  - The Remote Connections dialog box is displayed.
- 2. Click the **Authentication** tab, and select the authentication type.

The following authentication options are displayed:

- · Imprivata Configuring Imprivata OneSign server.
- · Caradigm—Configuring Caradigm server.
- SECUREMATRIX— Configuring SECUREMATRIX.
- HealthCast—Introduction to HealthCast.



3. After configuring your preferred authentication, click  $\mathbf{OK}$  to save the settings.

### **Configuring Imprivata OneSign server**

OneSign Virtual Desktop Access provides a seamless authentication experience and can be combined with single sign-on for No Click Access to desktops and applications in a virtual desktop environment.

To configure the OneSign Server, enter the details of the OneSign Server (either https://ip or https://FQDN values), reboot the client to display the logon dialog box, and then enter credentials to open the VDI broker dialog box for logon use. You can also set this feature in your INI file, see *Dell Wyse ThinOS INI Reference Guide*.

The following OneSign features or actions are supported:

- · Client and Broker authentication
  - o Citrix Virtual Apps (formerly Citrix XenApp)
  - o Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop)
  - VMware View
- Kiosk Mode

- Fast User Switching
- · Non-OneSign user VDI access
- · Hotkey Disconnect
- · Proximity card reader redirection
- · Guided Question and Answer login
- · Authenticate w/Password
- Authenticate w/Password + Password Change
- · Authenticate w/Password + Password Change | New Password is Invalid
- · Authenticate w/Proximity Card + Password
- · Authenticate w/Proximity Card + Pin
- Authenticate w/Proximity Card + Pin | Pin not enrolled
- · Authenticate w/Proximity Card Alone | Retrieve Password
- · Retrieve User Identity Password
- · Reset User Identity Password
- · Update User Identity Password
- · Enroll Proximity Card
- · Lock/Unlock Terminal with Proximity CardLock/Unlock Terminal with Proximity Card

ThinOS supports latest Imprivata WebAPI version 5. It includes OneSign Objects (WebAPI v4) and Fingerprint Authentication (WebAPI v5).

From ThinOS 8.3.1 Hot Fix release, Imprivata SSO solution is supported for ARM platforms—Wyse 3010 thin client and Wyse 3020 thin client series.

#### Configuring objects on Imprivata Server

Imprivata WebAPI is updated from version 4 to version 5. From earlier version, supports configuration objects are supported that enables you to control different aspects of client behavior. The Imprivata WebAPI feature is available on OneSign server 4.9 and later versions. The Configuration objects control different aspects of the client behavior.

Use the following guidelines to configure the objects on Imprivata Server:

- 1. Configuring the General configuration object
  - a. On the Imprivata server, click Computer policy, and then click General tab.
  - **b.** Select the check box to allow users to shut down and restart workstation from lock screen.
    - i NOTE: Display shutdown button and restarts commands to the user on the OneSign GINA.

The following configuration objects are supported on Imprivata server:

· Shutdown Allow

o If you enable this feature by selecting the check box, the **shutdown** and **restart** icon is shown in ThinOS login and locked



windows

- o If you clear the check box, the **shutdown** and **restart** icon is grayed out.
- FailedOneSignAuth Allow—Only yes or no options are supported. Non-OneSign user can log in to the Broker by clicking No radio button.
- · Logging Allow
  - o OneSign logs could output on ThinOS with this feature. An INI configuration is needed correspondingly.
  - o Loglevel=0/1/2/3. The default value is 0. If set to 0, logs are not displayed.
- Display name format— Account name can be shown correctly with different formats in pop-up notifications.

#### 2. Configuring the Walkway configuration object

On the Imprivata server, click Computer policy, and then click the Walk Away tab.

- Key mouse inactivity enabled and behavior The check box in addition to keyboard and mouse inactivity is not supported.
- · Passive proximity cards
  - o If you want to use proximity card to lock the computer, select the **Tap to lock** check box.
  - o If you want to lock the computer and log in as a different user. select the Switch users check box.
  - INI parameter is TapToLock=0/1/2.
- Lock warning enabled and type—The three types that are supported are: none, notification balloon and Screensaver.
  - o None—No warning messages are displayed.
  - o Notification balloon—ThinOS displays a notification window.
  - Screensaver—Hide the display contents before the workstation locks.
- · Warning message—The message can be customized.
- · Lock Screen type—Only obscure type is supported.
- Hot key to lock workstation or log off user—ThinOS can support following keys:
  - "F1 ~ F12", "BKSP", "DEL", "DOWN", "END", "ENTER", "ESC", "HOME", "INS", "LALT", "LEFT", "LCONTROL", "NUMLOCK", "PGDN", "PGUP", "RCONTROL", "RIGHT", RTALT", "SPACE", "TAB", "UP", "a~z", "A~Z", "0~9" and modifier "+", "%", "^" (Shift, Alt and Control)
- Suspend action—The server configuration controls this feature on ThinOS. Therefore a new INI is added— SuspendAction=0/1; 0 means lock, 1 means signoff.

#### 3. Configuring the SSPR Configuration Object

The SSPR configuration object controls the Self-Service Password Reset behavior for a user. The enabled attribute specifies whether the user is allowed to reset their password as part of emergency access. The mandatory attribute specifies whether the user must reset their password as part of emergency access.

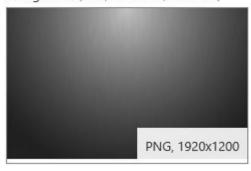
#### 4. Configuring the RFIDeas configuration object

The RFIDeas configuration object controls the behavior of the RFIDeas readers. The configuration can be configured by two ways, the computer policy of OneSign server and ThinOS INI.

#### 5. Configuring the Custom background configuration object

On the Imprivata server, click **Computer policy**, and then click the **Customization** tab.

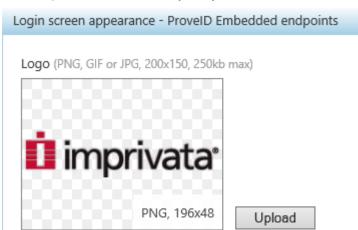




Upload

#### 6. Configuring the Co-Branding configuration object

On the Imprivata server, click Computer policy, and then click Customization.



Logo image impacts all the dialog boxes in ThinOS with raw logo.

#### 7. Configuring the SSPR Customization configuration object

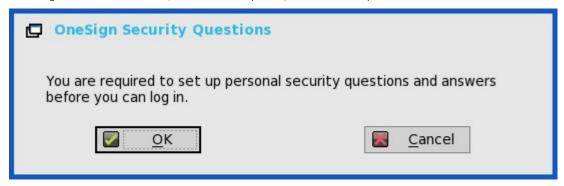
- · The text displayed in sign-on UI and lock window can be customized.
- The largest size supported by ThinOS is 17 characters.

ThinOS UI:



#### 8. Password Self-Services force enrollment feature

Selecting this check box allows you to reset the primary authentication password.



#### INI configuration for Imprivata OneSign Server

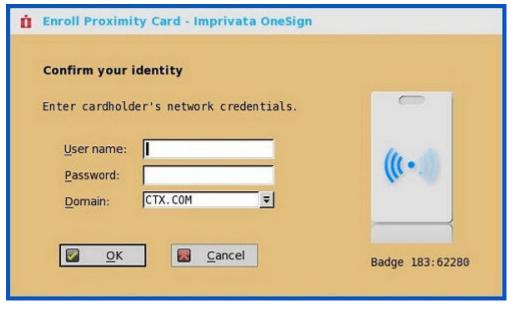
A new INI parameter AutoAccess=command is added. The new value is AutoAccess=Local. When AutoAccessis set to local, the ThinOS ignores the brokers that are set on the Imprivata OneSign Appliance and starts the broker/connections which are defined in wnos.ini or local defined on the client. You can start the vWorkspace, Microsoft, and other ThinOS connections while supporting Imprivata user authentication.

#### Proximity card enrollment

1. Tap the proximity card. The card enrollment page is displayed.



2. Enter the credentials and then click **OK**.



Proximity card is enrolled successfully.



#### Imprivata Bio-metric Single Sign-On

Fingerprint identification feature is highly reliable, and cannot be easily replicated, altered, or misappropriated.

The prerequisites of OneSign server are:

- · Imprivata v4.9 or later appliance version is needed that supports the WebAPI v5 and later versions.
- · Fingerprint identification license is required.

### (i) NOTE:

- Supported protocols are Microsoft RDP, Citrix ICA, PCoIP, and VMware Blast.
- Required Fingerprint reader devices are:
  - o ET710 (PID 147e VID 2016)
  - o ET700 (PID 147e VID 3001)

#### Supported scenarios

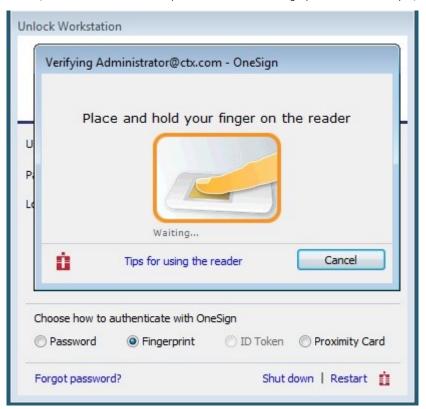
- 1. Signing in or unlocking the ThinOS devices using Fingerprint Authentication.
  - $\cdot$  Configure the OneSign server on ThinOS, and then plug-in the fingerprint reader device.
  - · The ThinOS Fingerprint window is displayed automatically after OneSign server is initialized.



· Fingerprint authentication works on the ThinOS unlock window.



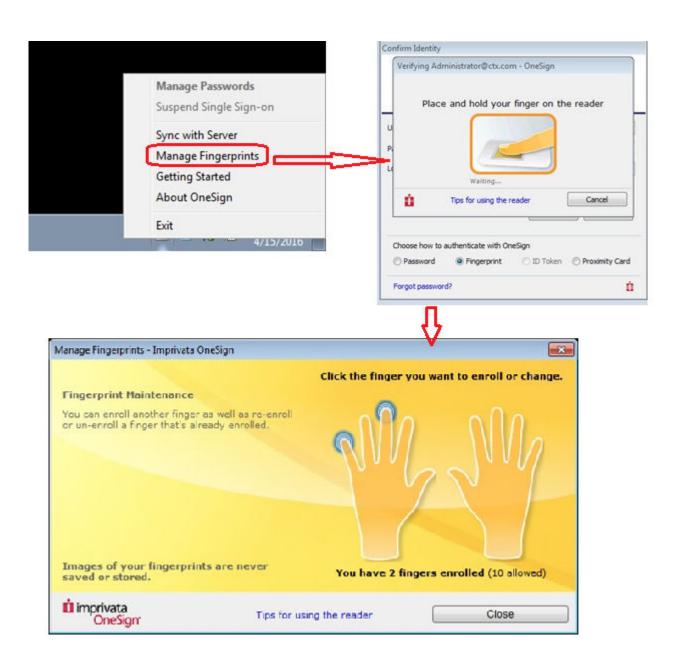
- 2. Unlocking the Virtual Desktop using Fingerprint Authentication.
  - · Enable the Imprivata Virtual Channel from the ThinOS Global Connection settings.
  - · When you lock the virtual desktop in the session, the Fingerprint window is displayed automatically.



- 3. Managing Fingerprints on virtual desktop.
  - · Legend Fingerprint Management is supported.
  - Fingerprint management with Imprivata Confirm ID enabled is not supported. This requires both supervisor and user to finish the enrollment and it is recommended to use Windows platform to perform this action.

To manage fingerprints, do the following:

- a. Right-click the OneSign agent icon in System tray.
- b. Click Manage Fingerprints, and enter the correct credentials in the displayed window to manage your Fingerprints.



#### Grace period to skip second authentication factor

Grace period enables you to specify a time limit on OneSign server for logging in without the second authentication factor after the first login session.

NOTE: After you specify the grace period, you must first use the proximity badge, and then enter password or OneSign PIN for the initial login.

If you use the proximity card after the time limit that you specified for grace period, the second authentication factor window is displayed with the message *Grace period expired*.



Figure 9. Second authentication factor window with the message

If you enter a wrong password or PIN, the second authentication factor window is displayed with the warning message OneSign could not authenticate you. Try again.



Figure 10. Second authentication factor window with the warning

### Use smart card as proximity card

You can use a smart card as a proximity card to authenticate the user. When you tap the smart card on the smart card reader, the Imprivata agent uses the smart card unique serial number as the Unique ID (UID) of the proximity card.

To use a smart card as proximity card, do the following:

- 1. Log in to the OneSign Administrator console.
- 2. Go to the Policies page and click Computer Policy.
- 3. In the Smart card readers section, select the Treat smart card authentications as proximity card authentications check box.

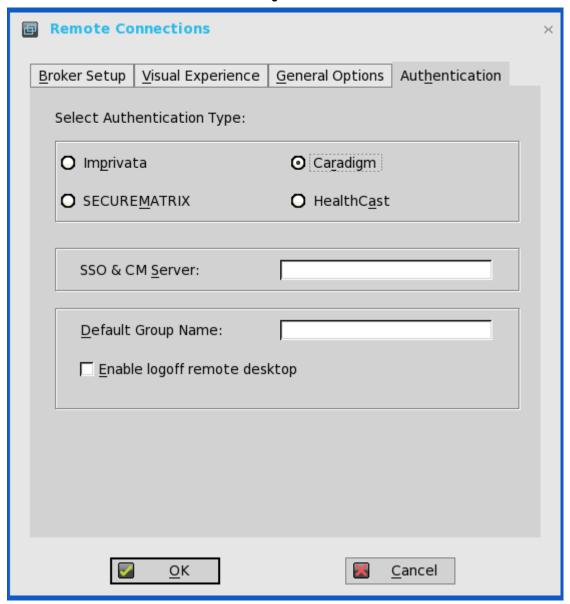
To authenticate the user using a proximity card, connect a supported reader to the thin client. Before you tap the card, ensure that your card is already enrolled to the user. When you tap your card on the reader, the thin client authenticates the user and starts the VDI connection.

### **Configuring the Caradigm server**

Caradigm Single Sign-on and Context Management (SSO & CM) is the product of the Caradigm Company which provides Single Sign-on and Context Management Services. Caradigm solution has been integrated since ThinOS 8.1.

To configure the Caradigm integration on ThinOS, do the following:

- From the desktop menu, click System Setup, and then click Remote Connections.
  The Remote Connections dialog box is displayed.
- 2. Click the Authentication tab, and then click Caradigm.



- a. SSO & CM Server—Enter the IP addresses of the Single Sign-On (SSO) and Context Management (CM) Servers.
- $\textbf{b.} \quad \textbf{Default Group Name} \\ \text{Type the name of the default group in the } \textbf{Default Group Name} \\ \text{box.}$
- c. Enable logoff remote desktop
  - · Select the check box to log off the current user from the session before system sign-off.
  - · Clear the selection to disconnect from the session.
- 3. Click **OK** to save the settings.

#### **Configuring the Caradigm Vault server**

To configure the Caradigm Vault server on ThinOS:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

- 2. Click the Authentication tab, click the Caradigm button, enter the IP address of the SSO & CM Server, and then click OK.
- **3.** On the Caradigm Vault Server, use the following guidelines:
  - Ensure that the **Enroll unenrolled badges** option is checked.
  - Make sure that all Badge ID mapping entries are deleted.

#### Tap Server

Way2Care Parameters	
Default Group Name	EGPGroup
Default Grace Period (min)	480
Badge Tap Processing Parameters	
Enroll Unenrolled Badges?	V
Badge Enrollment Timeout (sec)	300
Remote Desktop Tap Synchronization Timeout (sec)	120
Client Certificate Validation Parameters	
Reject Expired Certificates?	
Reject Self-Signed Certificates?	
Revoked Client Certificates	Revoke a Certificate
<< Click Revoke a Certificate to specify a Thin Client co	certificate that should be rejected >>
Client Certificate Filters	Add New Filter
<< Click Add New Filter to specify a filter for accept	ptable Thin Client certificates >>
Badge ID Mapping Parameters Add New Badge ID Mapping	
<< Click Add New Badge ID Mapping to specify a ma	
	Арр

4. Click SSO&CM > Advanced Configurations , and use the following guidelines:



- a. Ensure that the **Enable Proximity Support** check box is selected.
- $\boldsymbol{b.}$  Ensure that the  $\boldsymbol{Enable\ way2care}$  check box is selected.
- 5. To prepare a certificate to the Caradigm Vault Server, use the following guidelines:

The Caradigm Vault Server uses the certificate to validate the connection between the Tap Server and the thin client.

- **a.** To raise a request for the certificate:
  - The certificate should be issued by your Certificate Authority.
  - · Prepare the certificate in two formats:
    - o PFX format which has a private key.
    - o The other is PEM format which is text-based, Base64-encoded DER file. For Example, Caradigm.cer, Caradigm.pfx.
- **b.** To import a certificate to the thin client, use either of the following two options:
  - · Click System Setup > System tools > Certificates to import certificates from USB storage or file server.
  - · Use INI file to import certificate.

AddCertificate=client cert.pfx password=passpass

c. To add a certificate to Vault server:

#### Thin Client Certificates



Use the **Thin Client Certificates** page to add certificates for the thin client devices. The certificate must be a text in PEM format, that is, a text-based Base64-encoded DER file.

- · Open the DER cert file on Notepad.
- · Log in to the Vault Server Admin Console, and then click Appliance > Thin Client Certificates.
- · Copy the Notepad text to the Vault server

#### Configuration on VDI server and desktops

Caradigm solution of ThinOS supports the multi-types of VDI server such as VMware View Horizon 6, Citrix Virtual Apps 6.5, Citrix Virtual Apps and Desktops 5.6, and Citrix Virtual Apps and Desktops 7.6.

To configure the VDI server and desktop:

- · Install the Caradigm desktop components in the servers and desktops.
- · Indicate vault server IP, and then provide a valid security token.
- Add following lines to Service section of the \programdata\sentillion\vergence\Authenticator.ini
  configuration file.

TapServerIdentification=True
RemotePromptForPassword=Badge

- NOTE: At present, the following PCoIP enabled thin clients offer Caradigm SSO over PCoIP:
  - Wyse 3030 LT with PCoIP
  - Wyse 3040 with PCoIP
  - Wyse 5010 with PCoIP (D10DP)
  - Wyse 5040 AIO with PCoIP (5213)
  - Wyse 5060 with PCoIP

SSO and CM client installed on your VDI server and desktops must be upgraded to latest version 6.2.5 in order to support this feature.

#### Caradigm Way2Care

Way2Care is part of Caradigm Identity and Access Management (IAM) portfolio, and is designed to securely access patient information from multiple clinical applications.

In ThinOS version 8.6, a new INI parameter CaradigmServer=xxx UseWay2Care=yes is added to support Way2Care. You can also set DisableManualLogon=yes EGPGroup=xxx along with the Caradigm Server parameter. This feature uses Way2Care API that is different from the TapServer API. Way2Care uses the decimal UID format.

For more information about the INI parameter, see the Dell Wyse ThinOS Version 8.6 INI Reference Guide at www.dell.com/support.

For more information about the Caradigm Way2Care feature, go to www.caradigm.com.

### **Configuring SECUREMATRIX**

SECUREMATRIX enhances the security of enterprise and cloud-based applications while providing seamless end user experience for a one-time password (OTP) that can be used for authentication with desktops, Windows, VPNs, intranets, extranets, web servers, e-commerce and other network resources.

To configure the **SECUREMATRIX Server**, enter either https://ip or https://FQDN values, reboot the client to display the **log on** dialog box, and then enter credentials to open the **VDI broker** dialog box for logon use. You can also set this feature in your INI file, see Dell Wyse ThinOS INI Guide. For details see SECUREMATRIX documentation.

#### Introduction to HealthCast

HealthCast Single Sign-On (SSO) solution is designed to improve user convenience, streamline workflow, and strengthen security compliance in demanding environments. The same proximity cards used for physical access are used to tap-in and tap-out of unique user sessions and to tap-over any sessions unintentionally left open on the ThinOS devices. Typically, you must type in your password only one time each day and use your proximity cards to streamline workflow and save time as they move between shared computers securely. Also, proximity cards can be secured with a PIN, if configured by the organization. The HealthCast SSO solution also supports user self-service password reset so that you can reset your own passwords without the need to call the help desk.

NOTE: HealthCast SSO Solution on ThinOS is a client-server solution. ThinOS provides the client-side functionality, but you must also install and configure the HealthCast Server components on a server system in order for the solution to work properly. Contact HealthCast on HealthCast website for one or more server installation executables, server requirements, and configuration information.

#### Configuring HealthCast on ThinOS

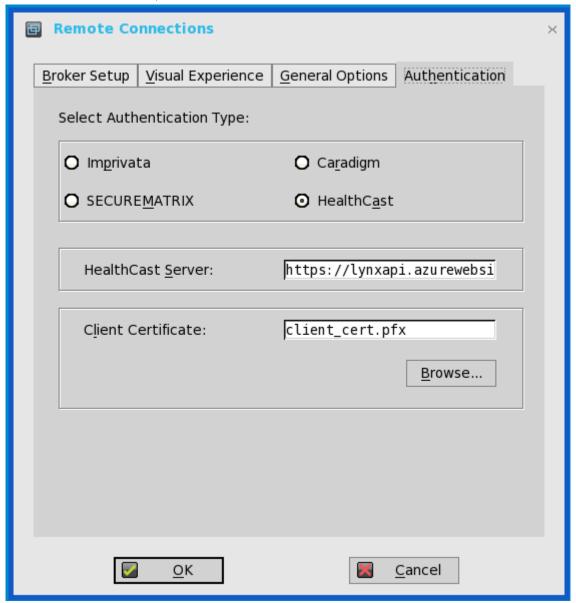
HealthCast Web API Server is integrated with ThinOS release to implement the HealthCast SSO solution. To use the HealthCast SSO solution, ThinOS must be configured to use the HealthCast Web API Server. You can do this by using the INI file (wnos.ini), or using the ThinOS UI. Dell recommends you to use the INI file for large deployments.

ThinOS UI configuration

- · To use the HealthCast Web API, configure the HealthCast settings on the thin client side. To configure, do the following:
  - 1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

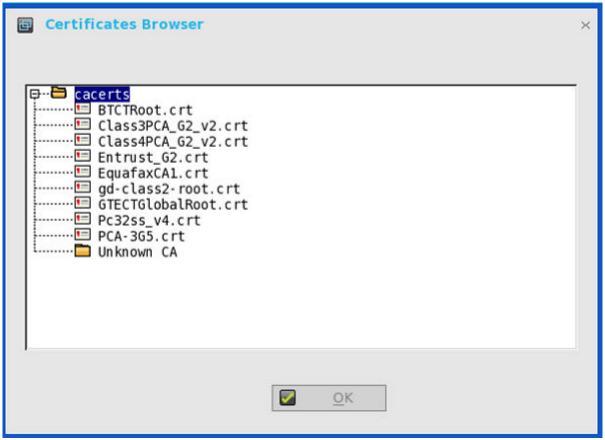
The **Remote Connections** dialog box is displayed.

2. Click the Authentication tab, and then click HealthCast.



3. Enter the HealthCast server details in the box provided.

4. To import the client certificate, click Browse, and select the appropriate certificate you want to use.



5. Click **OK** to save the settings.

INI configuration

To configure using INI parameters, add the following INI parameters to your wnos.ini file:

HealthCastServer— The server address and options needed for the client to connect to the HealthCast Web API Server.
HealthCastServer=<a href="https://doi.org/10.2016/j.com/">https://doi.org/10.2016/j.com/</a> SecurityMode=<default, full, warning, low>
ClientCertificate=<cert-pfx-file-name>

For example: HealthCastServer=https://server1.example.com SecurityMode=full ClientCertificate=client-cert.pfx.

For more information on INI parameters, see Dell Wyse INI Reference Guide.

#### HealthCast SSO features and functionality on ThinOS

The following are the HealthCast SSO features and functionality on ThinOS:

• **Proximity card enrollment**—HealthCast supports user self-enrollment. Therefore, there is no need to bring the proximity card to a special registration station, or for IT staff to be involved. Instead, you must only tap the disenrolled proximity card at a terminal and you

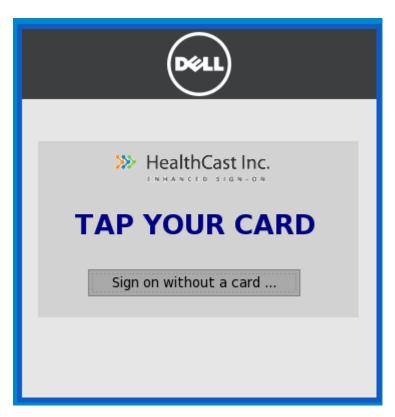
can follow the easy registration process. This is a one-time event after which you can use the card wherever HealthCast is installed.



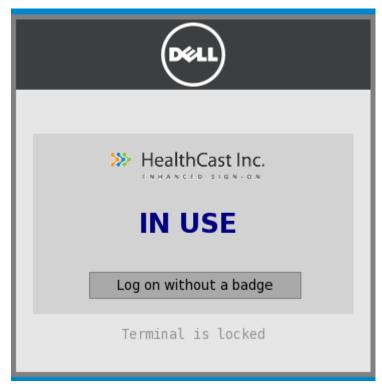
Manual login and lock/unlock terminal—If you do not have a card, or choose not to use your card, then you can manually log in using your user name and password. Administrators can disable manual login, if they wish, so that users can sign on with their proximity cards. You can also lock or unlock the terminal, if you have signed on with a manual login.



• **Proximity card login and lock/unlock terminal**—After the proximity card is registered, tap the card at a terminal to login.



You can lock the session to secure it, but leave the remote session connected for fast access when you return. To do this, tap the proximity card and the session is locked.



To resume the session, tap the card again.

- Walk away—Terminals can be configured to lock or log off sessions that have been left open. The time that will elapse before automatic lock or log off can be set by an administrator using the convenient web administration application.
- **Tap-Over**—If a session is locked or left open, a second user can tap their own proximity card and this will disconnect the first session and log the second user into their own unique session.
- Forgotten card—If you forget your card at home, you can receive a temporary card and register it for the day using the same easy registration process mentioned in this section.

- Lost or stolen card—If you report a card as lost or stolen, an administrator can immediately disable the card using the convenient
  web administration application. This prevents anyone else from using it.
- Self-Service Password Reset (SSPR)—If SSPR enabled by an administrator, you can register for SSPR and reset your passwords
  without calling the help desk.



• **Easy to use web-based administration tool**—Administrators can quickly and easily configure settings, manage proximity cards, and users using a web-based administration tool.

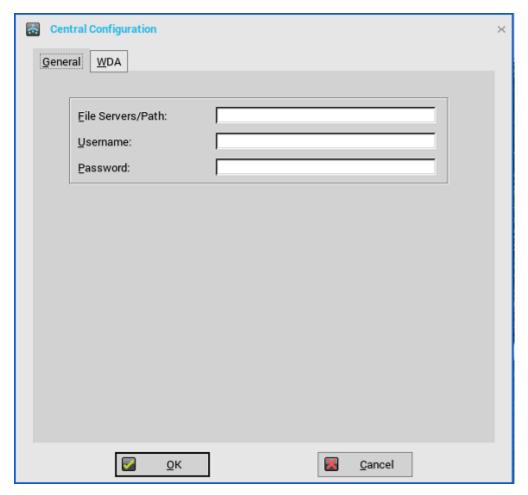
# Configuring the central configurations

Use the **Central Configuration** dialog box to configure the file server, WDM server settings, and Wyse Management Suite server settings.

# Configuring the general central configurations

To configure the general central configurations:

- From the desktop menu, click System Setup, and then click Central Configuration.
   The Central Configuration dialog box is displayed.
- 2. Click General tab, and use the following guidelines:



**File Servers/Path**, **Username**, and **Password**—Enter the IP address or hostname of the file server that provides the system software and update images. The address can be supplied through DHCP, if DHCP is used.

- i NOTE: It is recommended to use HTTPS instead of FTP or HTTP as it is a secure connection.
- **a.** File Servers/Path—Allows maximum of 127 characters for file server, and maximum of 127 characters for root path. The data specifies part of the path to be used when the server is accessed.
  - File server supports failover list. A failover list consists of one or more file server pairs specified in the order of preference. You can provide multiple file servers separated by either a semicolon or colon. The list must not exceed 127 characters. When connecting to a file server, the client attempts to connect to each pair in an order until it finds a working file server pair. It is recommended to limit the file server directory access to administrators.
- **b. Username**—Enter the username to log in to the file server. Use maximum of 31 characters.
  - NOTE: If you use an FTP connection with Anonymous login, a warning message is displayed, recommending to use a user-specific username. This warning message is also added in the event log.
- c. Password—Enter the password to log in to the file server. Use maximum of 31 characters.
- 3. Click **OK** to save the settings.

# **Configuring the Wyse Device Agent settings**

Use this tab to configure the Wyse Device Manager and Wyse Management Suite settings.

ThinOS supports all the Wyse Management Suite Group Policy settings.

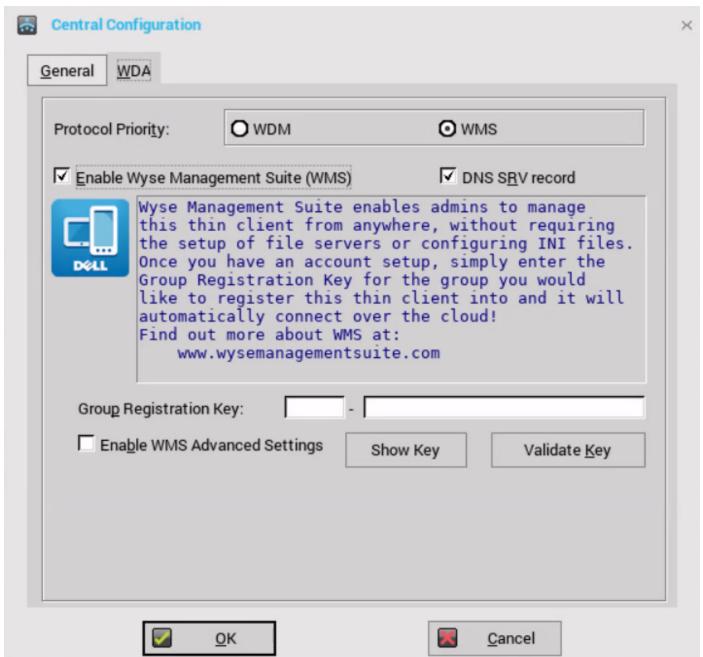
Dell Wyse Device Agent (WDA) has been enhanced to support the following three types of customer security environments:

Highly secured environment—Administrators must log in to each device, and use the USB device or File Server to import the
server certificate. The server certificate is retained in the device until you reset the device to factory default settings. The device is
secured and is not susceptible to a rouge DHCP or DNS server for a new device discovery. Administrators can use either CA-signed or
self-signed server certificates.

- Secured environment—Administrators can configure the server certificate fingerprint as a DNS\_Text record or a DHCP\_Scope option. If WDA detects the DNS\_Text record or the DHCP\_Scope option, the server certificate fingerprint is distributed over the network and added locally to the device. When the device is reimaged, the server certificate fingerprint is removed from the device. Administrators can use either CA-signed or self-signed server certificates.
- Normal environment—You can use either CA-signed or self-signed server certificates for device discovery. The device must
  establish a connection with CA for certificate validation. This applies when there is no option of DNS\_Text record or DHCP\_Scope but
  the server certificate is CA-signed. If the certificate is a self-signed certificate, you must accept the certificate security warning
  message.

To configure the Wyse Management Suite settings, do the following:

- From the desktop menu, click System Setup, and then click Central Configuration.
   The Central Configuration dialog box is displayed.
- 2. Click WDA > WMS, and use the following guidelines:



By default, the **WMS** option is selected. Wyse Management Suite service automatically runs after the client boot up.

If the first discovery, for example, the Wyse Management Suite service is not successful, it seeks for the next priority, for example, WDM service. This continues until a discovery is successful. If all discoveries fail, it is started again automatically after a fixed time—24 hours.

- a. Enable Wyse Management Suite (WMS)—Select the check box to enable the Wyse Management Suite to discover your thin client.
- b. **DNS SRV record**—Select this check box if you want the thin client to obtain the Wyse Management Suite values through DNS server, and then try to register into the Wyse Management Suite server. By default, the check box is selected. If the check box selection is canceled, the thin client cannot obtain the Wyse Management Suite values through DNS server.

To create DNS records in DNS server, use the following information:

# WMS server URL

DNS Record Type: DNS SRV

Record Name: WMS MGMT. TCP. < Domain>

Value Returned: WDMNG Server URL

Example: \_WMS\_MGMT.\_TCP.WDADEV.com

# MQTT Server URL

DNS Record Type: **DNS SRV** 

Record Name: WMS MQTT. TCP. < Domain>

Value Returned: WMS Server URL

Example: WMS MQTT. TCP.WDADEV.com

# Group Token

DNS Record Type: DNS Text

Record Name: WMS GROUPTOKEN. < Domain>

Value Returned: **Group Token** (as String)

Example: WMS GROUPTOKEN .WDADEV.com

# CA Validation

DNS Record Type: DNS Text

Record Name: WMS CAVALIDATION. < Domain>

Value Returned: TRUE or FALSE (as String)

Example: \_WMS\_CAVALIDATION.WDADEV.com

c. Group Registration Key—Enter the Group Registration Key as configured by your Wyse Management Suite administrator for the desired group. To verify the key, click Validate Key.

To view the specified group token key, click the **Show Key** button. Verify whether the specified group token key is correct. You can also press the F5 key to display the group token. When you press other keys on the keyboard, the group token is masked automatically.

- NOTE: A Group Registration Key is not required for the private Wyse Management Suite server. You can provide the Wyse Management Suite server details to enable the device to check in to Wyse Management Suite. ThinOS registers to a quarantine tenant in Wyse Management Suite.
- d. **Enable WMS Advanced Settings**—Select this check box to enter the Wyse Management Suite server, MQTT server details, and to enable the CA validation. By default, the MQTT server option is disabled. The MQTT server value is populated after the ThinOS device is checked in to the Wyse Management Suite.
  - NOTE: If you enable the Wyse Management Suite, ensure that you have entered the Group Registration Key and configured the Wyse Management Suite advanced settings.

The **CA validation** is required when you import certificates into your Wyse Management Suite server. By default, the CA Validation check box is selected to improve the security when using the Wyse Management Suite cloud. This change affects connections to any of the following servers:

- \*.dellmobilitymanager.com
- \*.cloudclientmanager.com
- \*.wysemanagementsuite.com

Table 9. CA validation

Wyse Management Suite deployment	CA Validation
Private cloud	When you deploy Wyse Management Suite on a private cloud, the <b>Enable CA</b> Validation check box is available to configure after you specify the server details in the  WMS Server field. By default, the check box is selected.
Public cloud	When you deploy Wyse Management Suite on a public cloud, the <b>Enable CA Validation</b> check box is selected by default. You cannot disable the <b>Enable CA Validation</b> option.

For more information about using Wyse Management Suite to manage the ThinOS devices, see the Wyse Management Suite Administrator's Guide at <a href="https://www.dell.com/manuals">www.dell.com/manuals</a>.

#### 3. Click **OK** to save the settings.

When you modify the ThinOS policy of the registered thin client using Wyse Management Suite, a dialog box is displayed prompting you to postpone or restart the thin client. To apply the settings immediately, click **Restart Now**. If you want to delay this task, click **Postpone**.

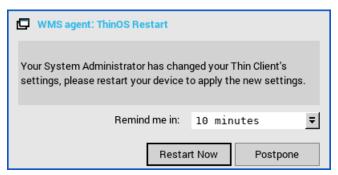
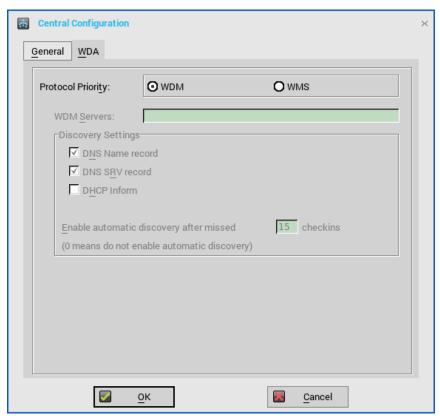


Figure 11. Wyse Management Agent: ThinOS restart

To configure the WDM settings, do the following:



1. Click WDM, and use the following guidelines:

- a. WDM Servers—If WDM is used, enter the IP addresses or host names. If user INI profiles are used, locations can be supplied through user profiles.
- b. DNS Name Record—(Dynamic Discovery) Allows devices to use the DNS hostname lookup method to discover a WDM server.
- c. DHCP Inform—(Dynamic Discovery) Allows devices to use DHCP Inform to discover a WDM server.
- d. Enable Automatic Discovery After Missed Check-ins—Select the number of missed check-ins after which you want the auto discovery options enabled.
- 2. Click **OK** to save the settings.

The Wyse Device Manager option can be disabled using the following INI parameters:

- · WMSService=no
- · Service=wdm disable=yes
- · RapportDisable=yes

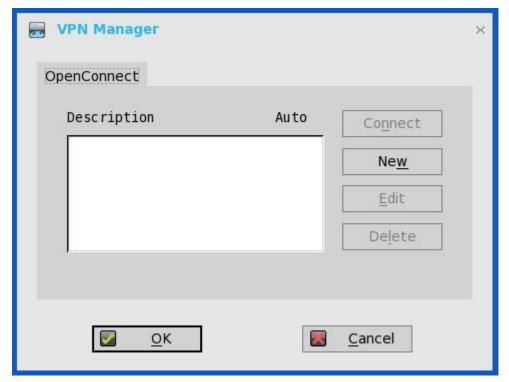
# Configuring the VPN Manager

VPN Manager is included to manage Virtual Private Network connections. ThinOS uses the OpenConnect client that is based on SSL protocol for connecting to VPN. A virtual private network (VPN) extends a private network across a public network such as the Internet. It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if the devices are directly connected to the private network, while benefitting from the functionality, security and management policies of the private network.

To configure the VPN Manager, use the following guidelines:

- In Classic Mode, from the desktop menu, click System Setup > VPN Manager.
   In Zero Mode, user can view the VPN Manager tab in System Settings panel.
- 2. Click VPN Manager.

The VPN Manager dialog box is displayed.

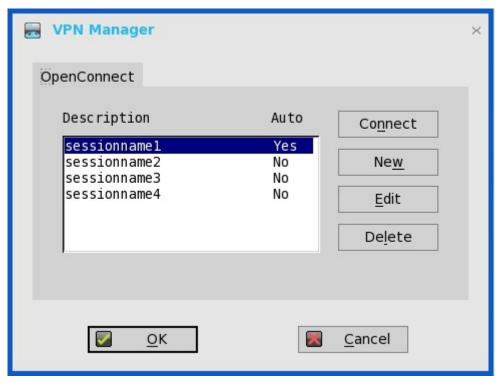


- 3. Click **New** to create a new session.
  - **a.** Session Name (up to 21 characters)—Enter the name of the Session Name. This is not a mandatory option. If the field is left blank, the VPN server name will be used as the session name.
  - b. VPN server (up to 63 characters)—Enter the IP address of the VPN Server. This is defined as either an IP address or a host name. This is a mandatory option.
  - c. Login Username (up to 31 characters)—Enter the Login Username. This is a mandatory option.
  - d. Login Password (up to 31 characters)—Enter the password of the user. This is not a mandatory option.
  - e. Select the check box to Auto-connect on system startup.

- f. Select the check box to show progress in detail.
- g. Click OK.



When the connections are created, the description column lists the session name and the Auto column shows which connection is automatically connected when the unit restarts. Only one session can be set to auto-connect.



#### 4. Click Connect.

The connection status is displayed.

# Configuring the connection brokers

In a Virtual Desktop Infrastructure (VDI) environment, a connection broker is a software entity that allows you to connect to an available desktop. The connection broker facilitates the VDI environment to securely and efficiently manage the centrally hosted desktop environments.

### (i) NOTE:

- Linux hosted desktop in Citrix, VMware, and Dell vWorkspace brokers are supported.
- Multimedia redirection (MMR) is not supported when you use RDP protocol to connect Windows 10 VM created in Microsoft RDS.
- Multimedia redirection (MMR) is supported when you use RDP protocol to connect Windows 10 VM created in Citrix Xen or VMware View.
- ThinOS does not support ICA multicast over VDMM.
- ThinOS supports ICA multimedia URL redirection (QUMU).
- ThinOS does not support Browser Content Redirection (HTML5 Redirection v2).

# **Configuring Citrix**

Citrix offers a complete virtualization solution, where all applications and resources are deployed on a centralized server, and published to remote devices. The Citrix Receiver client software installed on the thin client allows you to interact with the application GUI, while all of the application processes are performed on the server.

This section provides information about how to configure a Citrix broker connection on your ThinOS device, and other Citrix features that you can configure on ThinOS.

### **Configuring the Citrix broker connection**

To configure the Citrix broker setup:

- 1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
  - The **Remote Connections** dialog box is displayed.
- 2. In the Broker Setup tab, from the drop-down list, select Citrix Xen, and do the following:
  - · Select the check box to enable the StoreFront style.
  - Broker Server— Enter the IP address/Hostname/FQDN of the Broker Server.
  - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semi-colon, and is case-sensitive.
  - · Select the check box to enable automatic reconnection at logon.
    - NOTE: If you enable the automatic reconnection, you are able to select from the reconnection options. Click either of the options where you can connect to the disconnected sessions only or connect to both active and disconnected sessions.
  - · Select the check box to enable automatic reconnection from the button menu.
    - (i) NOTE: If you enable the automatic reconnection, you are able to select from the reconnection options. Click either of the options where you can connect to the disconnected sessions only or connect to both active and disconnected sessions.
  - · Account Self-Service Server— Enter the IP address of the Account self-service server.
  - XenApp Use this option, if you want to set default settings to XenApp.
  - XenDesktop— Use this option, if you want to set default settings to XenDesktop.
- 3. Click **OK** to save the settings.

# Citrix Receiver feature matrix

Table 10. Citrix Receiver feature matrix

	Features	Operating System—ThinOS	
	Citrix Virtual Applications	Supported	
	Citrix Virtual Apps and Desktops	Supported	
	Follow Me Apps/Subscriptions	Supported	
	Offline Apps (App V)	Not applicable	
Content	File Open in Receiver	Not applicable	
	Desktop Viewer/Toolbar	Not supported	
	Multitasking	Supported	
	Follow Me Sessions (Workspace Control)	Supported	
	URL Redirection	Not supported	
	Audio Playback	Supported	
	UDP Audio	Supported	
	Bidirectional Audio (VoIP)	Supported	
	Web Cam (Video Chat)	Supported	
	Video Playback	Supported	
	Flash Redirection	Supported (x86 only)	
	Skype for business Optimization pack	Supported (x86 only)	
	Cisco Jabber Unified Communications Optimization	Supported (x86 only)	
	Windows Multimedia Redirection	Supported	
	Local Printing	Supported	
H.264-enhanced SuperCodec		Supported	
	Adaptive Transport	Limited support <sup>1</sup>	
HDX	Framehawk	Not supported	
	Client hardware acceleration	Limited support	
	Desktop Composition redirection	Not supported	
	3DPro Graphics	Supported	
	Remote FX	Not supported	
	Location-Based Services	Not supported	
	Client drive mapping/File Transfer*	Supported	
	Generic USB redirection	Supported	
	SDWAN Support	Verification needed	
	Local App Access	Not applicable	
	Multi-touch	Not supported	
	Mobility Pack	Not applicable	
	HDX Insight	Supported	

Table 10. Citrix Receiver feature matrix (continued)

Features		Operating System—ThinOS
	Experience Metrics	Supported
	External Monitor	Supported
	True Multi Monitor	Supported
	Session Sharing	Supported
	Session Reliability	Supported
	Auto Client reconnect	Supported
	Multi-port ICA	Supported
	Receiver for Web Access	Not applicable
	Remote Access via NetScaler Gateway	Supported
	NetScaler Full VPN	Supported
	RSA Soft Token	Supported
	Challenge Response SMS	Supported
	User Cert Auth via NetScaler Gateway	Supported
	Smart Card (CAC, PIV and so on)	Supported
Security and communication	Proximity/Contact less Card (Fast Connect)	Supported
	Pass Through Authentication	Supported
	SAN Cert	Verification needed
	SHA2 Certs	Supported
	TLS 1.1/1.2	Supported
	AES and 3DES Encryption	Supported
	Smart Access	Supported
	IPv6	Supported
Updates	Auto Discovery/Configuration	Not supported
Opuates	App Store Updates/Citrix updates	Not supported

<sup>\*</sup>File transfer feature applies to HTML5/Chrome Receiver only.

For more information about Citrix Receiver features, see the Citrix documentation at www.citrix.com.

# Citrix HDX RealTime Multimedia Engine or RealTime Optimization Pack

HDX RealTime Optimization Pack (RTOP) provides a scalable solution to deliver audio-video conferencing and Voice over Internet Protocol (VoIP) enterprise telecommunication by using Microsoft Skype for Business. The Optimization Pack supports XenDesktop and XenApp environments to users on ThinOS devices. For more information about HDX RealTime Optimization Pack, see Citrix documentation.

<sup>&</sup>lt;sup>1</sup>Adaptive transport is a data transport mechanism for Citrix Virtual Apps and Desktops. This mechanism enables the underlying protocol to switch between the Citrix protocol called Enlightened Data Transport (EDT) and Transmission Control Protocol (TCP) for better performance. EDT is added on top of UDP and enhances the data throughput for all ICA virtual channels. ThinOS supports adaptive transport using Transmission Control Protocol (TCP), and does not support adaptive transport through User Datagram Protocol (UDP) except the audio channel. For more information about Adaptive transport, see docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview/hdx/adaptive-transport.html.

This section provides information about supported platforms for RealTime Multimedia Engine (RTME), installation of RTME package, Citrix remote server/Desktop host preparation, configuration on ThinOS, and RTME status check and troubleshooting.

#### Introduction

Citrix HDX RealTime Optimization pack offers high-definition audio and video calls. In every ThinOS release, the RTME version may be updated to newer version.

For more information about the Citrix RTME 1.8 feature, see the HDX RealTime Optimization Pack article at docs.citrix.com.

For more information about the Citrix RTME 2.x feature, see the latest RealTime Optimization Pack article at docs.citrix.com.

#### Supported environments

- · Citrix environment: Citrix Virtual Apps and Desktops 5.6/6.5/7.x.
- Desktop with RTME connector 1.8 (Lync server and client version 2010 and 2013; Skype for Business client in Lync 2013 GUI is supported).
- · Desktop with RTME connector 2.x (Both Skype for Business 2015 and Skype for Business 2016 are supported).
- · Supported networks: LAN, WAN (VPN), wireless and so on.
- · Supports calls between RTME clients or between RTME and standard Lync clients.
- · Supports Microsoft Office 365 or Skype for Business Online. For more information, See the Citrix documentation.

#### RTME supported platforms

- Wyse 5010 with ThinOS (D10D), Wyse 5010 thin client with PCoIP (D10DP)
- Wyse 3030 LT thin client with ThinOS, Wyse 3030 LT thin client with PCoIP
- · Wyse 3040 thin client with ThinOS, Wyse 3040 thin client with PCoIP
- · Wyse 5060 thin client with ThinOS, Wyse 5060 thin client with PCoIP
- · Wyse 5040 AlO thin client with ThinOS (5212 AlO), Wyse 5040 AlO thin client with PCoIP (5213)
- · Wyse 5070 thin client with ThinOS, Wyse 5070 Extended thin client with ThinOS, Wyse 5070 thin client with PCoIP
- · Wyse 7010 thin client with ThinOS (Z10D)

### Installing RTME package on ThinOS

You are required to install the RTME.i386 package for the RTME feature to work on ThinOS.

To install the RTME.i386 package:

- 1. Upload the RTME.i386.pkg to directory \wnos\pkg\.
- 2. You must ensure that the INI autoload is not set to value 0.
- **3.** Restart the thin client and wait till the auto-installation of packages is complete. The installed RTME package is displayed in the **Packages** window in System Tools.

### Setting up the RealTime Multimedia Engine connector

This section describes how to install and use Lync or Skype for Business (SFB) on a Citrix desktop.

- 1. Install Citrix HDX RealTime Connector on Citrix desktop VDA/Server. HDX RealTime Multimedia Engine (RTME) is the package installed on ThinOS. It is HDX RealTime Connector that needs to be installed or upgraded on the remote server and VDA.
  - NOTE: The following are applicable to RTME 1.8 only:
    - The Upgrade option from 1.7 to 1.8 is discussed at docs.citrix.com/en-us/hdx-optimization/1-8/upgrade-1-7-to-1-8.html.
    - The Firewall configuration is required on remote server and VDA. For more information, refer to docs.citrix.com/en-us/hdx-optimization/1-8/hdx-realtime-optimization-pack-configure-firewall.html.
    - The RTME 1.8 feature on ThinOS supports only HDX RealTime Connector 1.8 due to Citrix limitation.
- 2. Update the ThinOS firmware, and install the RTME.i386.pkg on the ThinOS client.
  - NOTE: Since ThinOS 8.3.1 HF release, the RTME 1.8 and 2.1 co-exist in the release package, supporting both versions of RTME connectors. In every ThinOS release, the RTME version may be updated to newer version and the latest RTME version co-exists with RTME 1.8 version in the corresponding release packages.
- 3. (This step is for RTME 1.8 only) Configure the Domain Name Server (DNS) settings on ThinOS for Lync Server.

# NOTE: You must ensure that the thin client does not have USB redirection for video/audio devices in order to have RTME working correctly.

- 4. Log in to your Citrix Desktop, and sign in to Lync client or Skype for Business (SFB) client.
  - · For RTME 1.8, the RTME icon is displayed in the lower-left corner of the Lync client window.
  - For RTME 2.x, the RTME icon is displayed on taskbar.

Use the Lync Application or Skype for Business application to perform the following tasks:

- Start an audio or video call
  - Select user to call
  - o Call from the IM window
  - o Type a name or number to call
- Answer the call
  - o Audio call
  - o Video call
  - Headset button to answer the call
- Transfer call/ mute/ hold call
- · Control the video: Pause/ End/ Picture in Picture (PiP)
- · Set the volume levels
- · Use Dial Pad
- · Make a conference call
- · Help and Hang up
- · Minimize/maximize or close the call video window
- · Perform Network Health check:
  - For RTME 1.8, press **Ctrl+N** to open the **Network Health** window.
  - o For RTME 2.x, right-click the RTME icon on taskbar and select Call Statistics.

The attributes, such as received packets, sent packets, video frame rate, video resolution, audio codec, and video codec are displayed in the above described window.

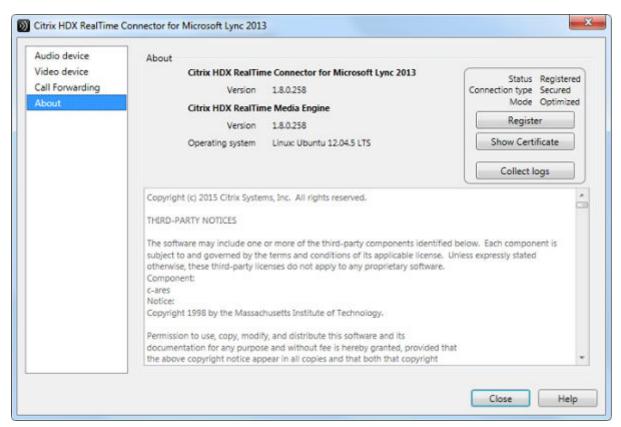
### Verifying the RTME 1.8 status

The Citrix HDX RealTime Connector for Microsoft Lync 2013 dialog box enables you to verify the RTME 1.8 status.

To view the Citrix HDX RealTime Connector for Microsoft Lync 2013 dialog box:

- 1. Do any of the following to view the Citrix HDX RealTime Connector for Microsoft Lync 2013 dialog box:
  - · Click the RTME icon in the lower-left corner of the Lync application window, and click Audio Video Settings.
  - · Click the Lync menu icon in the upper-right corner of the Lync application window, and click Tools > Audio Video Settings.

The Citrix HDX RealTime Connector for Microsoft Lync 2013 dialog box is displayed.



2. Click the About tab in the Citrix HDX RealTime Connector for Microsoft Lync 2013 dialog box.

The RTME status is displayed in the upper-right pane of the dialog box. If the RealTime Multimedia Engine is successfully initiated between the ThinOS client and Citrix desktop, the RTME status is displayed as follows:

#### Table 11. RTME status

Attribute	Value
Status	Registered
Connection Type	Secured
Mode	Optimized

You can also view the Citrix HDX RealTime Connector for Microsoft Lync 2013 version and Citrix HDX RealTime Media Engine version in the dialog box.

- 3. Click the Audio Device tab to configure the RTME audio settings, such as speakers, microphone, and ringer settings.
  - (i) NOTE: The RTME audio device on ThinOS shows only one device from ThinOS local playback device. It can actually work the way they are configured at ThinOS local playback device and record device. The RTME audio device for ringtone is limited to use ThinOS local playback device. This is a known Issue.
- 4. Click the **Video Device** tab to configure the RTME video settings. From the drop-down list, select the webcam that you want to use for video calls.
- 5. Click the **Call Forwarding** tab to configure the call forwarding settings.

You can configure the following options:

- Turn off call forwarding
- · Forward any call to a specific number
- Simultaneously ring
- i NOTE: The latest call forwarding settings configured by you are displayed in the lower pane of the dialog box.

For more information about trouble shooting, go to docs.citrix.com/en-us/hdx-optimization/1-8/hdx-realtime-optimization-pack-troubleshooting.html.

For information about the tested devices for RTME, see the latest Dell Wyse ThinOS release Notes.

#### **Known issues**

- · RTME operation system on ThinOS is displayed as Linux.
- The RTME 1.8 feature on ThinOS does not work with other versions of HDX RealTime connector due to known Citrix limitation.
- · If you change the audio device during an RTME call, the audio input or output might stop responding.
- In a video conference call, when different user is speaking, the on-screen video switches to the active user, but takes a few seconds to switch over.

### Verifying the RTME 2.x status

This section describes the working of RTME 2.x and how to verify the RTME status.

#### Salient features

- · Native Skype For Business client menus and operations are available.
- · Better initialization eliminates DNS confusions.
- · Supports more call features, such as call delegation, and response group.
- · Supports video codec H.264-UC, and audio codec SILK introduced by RTME 2.1.
- · Call Admission Control support
- Bandwidth Policy Control
- · DSCP/ QoS Configuration
- · Ability to turn off version mismatch warnings for acceptable combinations of RealTime Connector and RealTime Media Engine.

To verify the RTME status, do the following:

- 1. Install the correct connector on the remote desktop.
- 2. Install the correct package on the ThinOS device.
- 3. Connect the audio or video devices.
  - i NOTE: USB redirection needs to be disabled for audio or video devices.
- 4. Connect to the remote desktop using SFB client.
- 5. Verify the RTME connector icon on taskbar. The status is displayed as Connected.
- 6. Verify the About and Settings option from the RTME connector menu.
- 7. Verify the audio/video devices from SFB client menus.
- 8. Establish the video/audio calls.
- 9. Pick up the calls by either clicking the mouse or using the headset button.
- 10. Verify the Call Statistics from the RTME connector menu.
  - NOTE: RTME 2.2 and later versions support various call scenarios. For more information, refer to Citrix documentation.

USB Video Class (UVC) 1.1 and 1.5 camera hardware encoding / H.264 (CAM) are supported in RTME 2.2 and later versions. This is applicable for qualified cameras only, for example Logitech C930e.

In the **Call Statistics** window, **Video Codec = H.264-UC (CAM))** is displayed for P2P RTME video call in the **Sent** column. For group calls with standard SFB, the call statistics displays **Video Codec = H.264-UC (CAM)** in the **Sent** column. This improves video call quality/resolution compared to Video Codec H.264 (SW); for example: P2P video call resolution upgrade from 480 x 270 to 640 x 360.

#### Limitations

- The video sent from client in call is decided by capabilities of both endpoints in the call. Sending higher video from one client does not mean that the client has better capability than the other one in call.
- $\cdot$   $\;$  RTME status dialog displays operation system as Linux.
- · Changing the video/audio device during RTME call results in issue with audio input or output.
- · Volume: Dell recommends you to adjust the speaker volume in audio settings of SFB client to high. By default, the SFB client audio volume is set to 40 percent. The default volume is a bit low.
- · Camera/Video: The local camera setting does not affect/impact the RTME video output because of the RTME design.
- In Citrix RTME version 2.3, the video performance of applications is designed for a lower CPU consumption. Therefore, the video resolution may be downgraded compared to version 2.2.

 ThinOS RTME package update does not support hardware acceleration. For more information, see the Citrix documentation at docs.citrix.com.

#### Citrix RTME call statistics

**Table 12. Citrix RTME call statistics** 

Platform name	RTME	Call statistics*			Camera
riationii name	version	Video resolution	Video codec	Video frame rate	Camera
Wyse 5470 Thin	2.7	1280 x 720	H.264-UC (CAM)	30	Logitech C930e
Client	2.7	960 x 540	H.264-UC (SW)	30	On-board camera
Wyse 5470 All-in-One	2.7	960 x 540	H.264-UC (SW)	30	On-board camera
Thin Client	2.7	1280 x 720	H.264-UC (CAM)	30	Logitech C930e
Wyse 5070 Thin Client	2.7	1280 x 720	H.264-UC (CAM)	30	Logitech C930e
Wyse 5060 Thin Client	2.7	848 x 480	H.264-UC (CAM)	30	Logitech C930e
Wyse 3040 Thin Client	2.7	848 x 480	H.264-UC (CAM)	30	Logitech C930e
Wyse 3030 LT Thin Client	2.7	848 x 480	H.264-UC (CAM)	30	Logitech C930e
Wyse 5010 Thin Client	2.7	424 x 240	H.264-UC (CAM)	15	Logitech C930e
Wyse 7010 Thin Client	2.7	424 x 240	H.264-UC (CAM)	15	Logitech C930e
Wyse 5040 AIO Thin Client	2.7	320 x 180	H.264-UC (SW)	15	On-board camera
Wyse 3020 Thin Client	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Wyse 3010 Thin Client	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

<sup>\*</sup>The call statistics data is displayed in the **Call Statistics** window in the **Sent** column.

### Cisco Jabber Softphone for VDI

Cisco Jabber Softphone for VDI (JVDI) is the Unified Communications solution offered by Cisco for virtual deployments. It supports audiovideo conferencing, and instant messaging on the hosted virtual desktops (HVD). The Cisco Jabber Softphone for VDI software offloads the audio or video processing from the virtual desktop servers to the thin client. All audio and video signals are routed directly between the endpoints without entering the HVD.

#### Introduction

Cisco Jabber Softphone for VDI enables you to make and receive calls using the Cisco Unified Communications application. Cisco Jabber Softphone for VDI consists of the following two components:

- · Cisco JVDI Agent
- · Cisco JVDI Client

Cisco JVDI Agent is the JVDI connector that runs on the Citrix desktop or server. Cisco JVDI client is the JVDI package that runs on the thin client. The Jabber client that runs on the Citrix server handles the authentication and the media processing is achieved on the thin client.

The JVDI PKG uses a major portion of the disk on platforms with low disk space. If you install JVDI PKG on thin clients with low disk space, other large PKGs may fail to extract and install. For example, you cannot install JVDI PKG, Horizon, and RTME PKG together on Wyse 5010 Thin Client. However, you can install the following PKGs together on Wyse 5010 and Wyse 5040 thin clients:

· RTME, FR, and JVDI

RTME, TCX, FR, and Horizon

This issue is not observed on thin clients with more disk space.

#### Supported environment

**Table 13. Supported environment** 

Component	Supported platforms/supported versions
Thin client	<ul> <li>Wyse 5070 Thin Client with ThinOS</li> <li>Wyse 5070 Thin Client with PCoIP</li> <li>Wyse 5060 Thin Client with ThinOS</li> <li>Wyse 5060 Thin Client with PCoIP</li> <li>Wyse 3040 Thin Client with ThinOS</li> <li>Wyse 3040 Thin Client with PCoIP</li> <li>Wyse 5010 Thin Client with ThinOS—only audio call is supported</li> <li>Wyse 5010 Thin Client with PCoIP—only audio call is supported</li> <li>Wyse 5040 AIO Thin Client with ThinOS—only audio call is supported</li> <li>Wyse 5040 AIO Thin Client with PCoIP—only audio call is supported</li> <li>Wyse 3030 LT Thin Client with ThinOS—only audio call is supported</li> <li>Wyse 3030 LT Thin Client with PCoIP—only audio call is supported</li> </ul>
Connection broker for the hosted virtual desktops	<ul> <li>Citrix Virtual Apps and Desktops (formerly XenDesktop) 7.15 LTSR and later</li> <li>Citrix Virtual Apps (formerly XenApp) 7.15 LTSR and later</li> </ul>
Cisco Jabber application on the hosted virtual desktop	Cisco Jabber 12.1
Cisco JVDI agent on the hosted virtual desktop	Cisco JVDI Agent 12.1
Cisco JVDI client on the thin client	JVDI.i386.pkg

### Installing the JVDI package on ThinOS

This section describes how to install the JVDI package on ThinOS. You must install the JVDI package to use Cisco Jabber Softphone for VDI.

To install the JVDI package:

- Extract the JVDI.zip package.
   The README WITH EULA.txt and JVDI.i386.pkg files are unzipped to a valid location.
- 2. Open the readme file and read the EULA agreement.
- **3.** Upload the JVDI.i386.pkg to directory \wnos\pkg\ on the file server.
- 4. Ensure that the value of the INI parameter autoload is not set to 0.
- **5.** Restart the thin client and wait until the automatic installation of packages is complete. The installed JVDI package is displayed in the **Packages** window in System Tools.

### Setting up the Cisco Jabber Softphone for VDI

This section describes how to install and use the Cisco Jabber Softphone for VDI on a Citrix desktop.

- 1. Go to www.cisco.com, and download the following software:
  - Cisco JVDI Agent 12.1
  - · Cisco Jabber application 12.1
- 2. On the Citrix virtual desktop, install Cisco JVDI Agent. Double-click the file and follow the installation wizard steps.
- 3. On the Citrix virtual desktop, install Cisco Jabber.
  - For information about the installation procedure, see the installation guide at www.cisco.com.
- **4.** Update the ThinOS firmware, and install the JVDI.i386.pkg on the ThinOS client. For more information about installing the JVDI package, see Installing JVDI package on ThinOS.

- NOTE: If ThinOS running Cisco Jabber (JVDI) fails to register with Cisco Unified Communications Manager, add the DNS servers and DNS domains that are used by the Citrix host and the Cisco Unified Communications Manager servers to ThinOS. You can either specify the domain name and server IP on the General tab in Network Setup, or add the DNS server and domain value to the DHCP server by providing the IP address information to the ThinOS client. For issues related to Cisco Unified Communications, contact the Cisco support.
- 5. Log in to the Citrix virtual desktop, and sign in to Cisco Jabber using your user credentials. When you log in for the first time, do the following:
  - a. On the Cisco Jabber interface, click Advanced Settings.
  - b. Select your account type as Cisco Communications Manager 9 or later.
  - c. Enter the login server address.

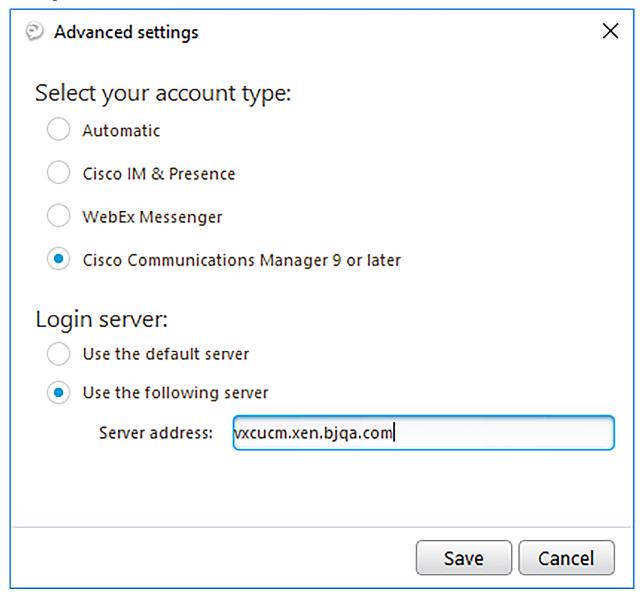


Figure 12. Advanced Settings

NOTE: If the Use my computer for calls option is selected, the Cisco Jabber is automatically registered with Cisco Unified Communications Manager. This option enables Jabber to work as a Softphone, and use the microphone or speaker that is connected to the thin client for phone calls.

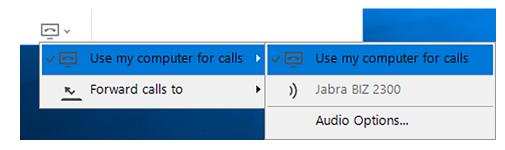


Figure 13. Use my computer for calls

#### **Using Device Selector**

Cisco Jabber Softphone for VDI consists of a component called **Device Selector**. Use the **Device Selector** menu to manage your audio devices and cameras.

If you have multiple devices connected to the thin client, you can view your active device, or select a different device. To enable a device, do the following:

In the Windows notification area, click the **Device Selector** icon.
 The available devices are listed.



Figure 14. Device Selector

2. Click a device to make it active.

#### **Using Cisco Jabber**

Use the Cisco Jabber application to perform the following tasks:

- · Start an audio or video call
- · Answer the call
- · Hold or resume the call
- Stop the video
- · Mute or unmute the audio
- · Turn on or turn off the self view
- Enter or exit the full screen
- Merge the calls
- · Audio conferencing

- · Transfer the call
- · Play voice mail
- · Forward the call to voicemail
- · Forward the call to another number
- · Forward voice messages directly
- · Use the Device Selector menu to switch between headsets
- · Use the Device Selector menu to switch between cameras
- · Set up secure phone capabilities
- · Answer the call on multiple phone devices (Shared Line feature)

### i) NOTE: Dell recommends that you reduce the video resolution to 640 x 360p with 30fps on Wyse 3040 thin client.

For information about the performance data statistics and limitations, see the *Dell Wyse ThinOS Version 8.6 Release Notes* at www.dell.com/support.

For information about troubleshooting your Cisco Jabber, see the *Deployment and Installation Guide for Cisco Jabber Softphone for VDI* at www.cisco.com.

For information about Cisco Jabber-related issues, see the *Release notes for Cisco Jabber Softphone for VDI* document at www.cisco.com.

For information about accessories for camera, headsets, and speakers, see the *Unified Communications Endpoint and Client Accessories* article at www.cisco.com.

#### Limitations

- · JVDI package cannot be installed on Dell Wyse 3030 LT, 5040, 5010, and 7010 thin clients.
- Dell Wyse 3040 thin client supports video call up to 360p. The video call with 720p is not supported due to high CPU cost with multimedia playback simultaneously. Dell recommends that you restrict the video up to 360p in the server settings.
- · Dell does not recommend video call in 4K display resolution on all platforms due to low performance.
- JVDI version in ThinOS 8.6 must be compatible with JVDI agent and Jabber version. For example, JVDI version 12.1 in ThinOS 8.6 supports JVDI agent and Jabber version 12.1.
- Audio output is poor when you enable the JVDI audio during the full screen video call on Wyse 5060 and 3040 thin clients. This is due
  to hardware performance limitation. Wyse 5070 thin client supports full screen video call with good audio output.

#### **Known issues**

#### Table 14. Known issues

Description	Workaround	
JVDI audio volume slider does not change the audio volume in Wyse 3040 thin client. This issue is due to Cisco Jabber limitation. For more information about the Cisco Jabber issues, see the <i>Release Notes for Cisco Jabber Softphone for VDI—Release 12.1</i> document at www.cisco.com.	Adjust audio volume by using either the ThinOS volume bar, session sound volume, or headset button.	
Self-camera or remote video does not work, or a black screen is displayed when you play a video. For more information about the Cisco Jabber issues, see the <i>Release Notes for Cisco Jabber Softphone for VDI—Release 12.1</i> document at www.cisco.com.	Sign out of the session or reboot the ThinOS client and register the JVDI again.	
ICA session cannot be launched and WdReceiv: trap 14 error occurs when you enable the ICA session reliability with multi-port in the JVDI environment.	Enable ICA session reliability without enabling multiport in JVDI environment.	
Answer/End/Hold options in headset do not work during the JVDI call.	You can Answer/End/Hold the call by using the Jabber application in the VDI session.	
DP audio does not work in JVDI. When you switch the DP audio in the JVDI device selector, the JVDI may re-register again and a redundant DP audio is listed in device selector. JVDI VXC process should not restart when you hotplug or turn off/on the monitor when using the DP audio in JVDI.	Sign out of the ICA session or reboot the ThinOS client. If you require DP audio, Dell recommends that you first set the DP audio in the ThinOS client and then launch the ICA session.	
Audio output is poor when you enable the JVDI audio during the full screen video call on Wyse 5060 and 3040 thin clients. This is due to the hardware performance limitation.	Use the JVDI video call with window mode on Wyse 5060 and 3040 thin clients.	

#### Table 14. Known issues (continued)

Description	Workaround
JVDI troubleshooting logs show incorrect information.	There is no workaround in this release.

#### Cisco Jabber call statistics

#### Table 15. Cisco Jabber call statistics on Wyse 5470 Thin Client

Citrix Apps and Desktops	VDI	Video resolution	Frame rate
7.15 LTSR	Windows 10 x64	1280 x 720p	25 fps

#### Table 16. Cisco Jabber call statistics on Wyse 5470 All-in-One Thin Client

Citrix Apps and Desktops	VDI	Video resolution	Frame rate
7.15 LTSR	Windows 10 x64	1280 x 720p	25 fps

### **Using Citrix ADC**

ThinOS supports Citrix application delivery controller (ADC), formerly known as Citrix NetScaler. The following authentication methods are supported on ThinOS:

- · Lightweight Directory Access Protocol (LDAP)
- · RSA
- · DUO
- · SMS PASSCODE
- OKTA

### Configuring Citrix NetScaler Gateway using LDAP and RSA

To configure the Citrix NetScaler Gateway using LDAP and RSA authentication, do the following:

- 1. Go to NetScaler > NetScaler Gateway > Virtual Servers, and click Edit.
- 2. Set the primary and secondary authentications based on the following scenarios:
  - · If you use LDAP and RSA login, ensure that the primary authentication is LDAP and secondary authentication is RADIUS.
  - · If you use RSA and LDAP login, ensure that the primary authentication is RSA and secondary authentication is LDAP.
  - · If you use only LDAP login, ensure that the primary authentication is LDAP and secondary authentication is none.
- 3. Add the following INI parameter in the wnos.ini file, and configure your file server: pnliteserver=<fqdn of NS Server> CAGAuthMethod={LDAP,LDAP+RSA,RSA+LDAP} Storefront={yes,no}

For more information about configuring Citrix NetScaler Gateway with LDAP, RSA authentication, see the Citrix NetScaler Gateway Guide at www.citrix.com.

### **Configuring Citrix NetScaler Gateway using DUO**

To configure the Citrix NetScaler Gateway using DUO authentication, do the following:

- 1. Go to NetScaler > NetScaler Gateway > Virtual Servers, and click Edit.
- 2. Ensure that the primary authentication is RADIUS that is configured with the DUO authentication RADIUS.
- **3.** Ensure that the secondary authentication is none.
- **4.** Add the following INI parameter in the wnos.ini file, and configure your file server: pnliteserver=<fqdn of NS Server> Storefront={yes,no}

For more information about configuring Citrix NetScaler Gateway with DUO authentication, see the Citrix NetScaler Gateway Guide at www.duo.com.

### Using Citrix NetScaler with CensorNet MFA authentication

SMS PASSCODE is re-branded as CensorNet MFA. You can configure NetScaler Gateway to use a One Time Passcode/Password (OTP) in the form of a personal identification number (PIN) or passcode. To obtain this one-time password, you must install CensorNet app on your mobile. After you enter the passcode or PIN, the authentication server invalidates the one-time password. You cannot enter the same PIN or password again. For more information about configuring one-time passcode, see the Citrix documentation.

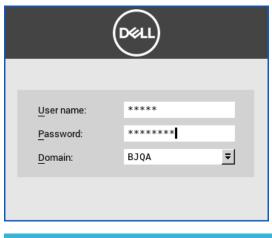
#### **Prerequisites**

- · NetScaler v12.0 and later is installed on your client.
- SMS PASSCODE v9.0 SP1 is installed and configured in your network. You can download the SMS PASSCODE v9.0 file from download.smspasscode.com/public/6260/SmsPasscode-900sp1.
- · Remote Authentication Dial-In User Service (RADIUS) authentication policy is configured and bind to the NetScaler gateway server.
- · CensorNet app is installed and configured on your mobile device.

To use the one-time passcode on ThinOS, do the following:

- 1. Log in to ThinOS, and connect to the NetScalar Gateway URL.
- 2. Enter your credentials (user ID and password), and press Enter.

  The PASSCODE dialog box is displayed. You will receive a push notification from the CensorNet App on your phone with the code.





### Message

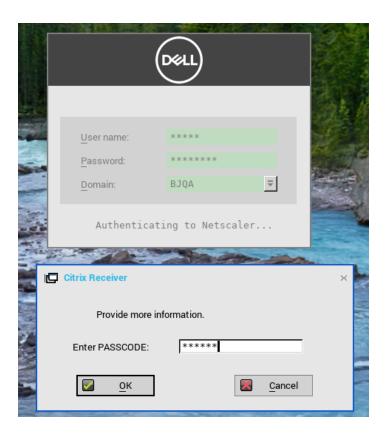
NON-TRUSTED LOCATION PASSCODE: ihyhyw Country: unknown Org: ???

Org: ??? Dell Wyse

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

#### 3. Click OK.

If the authentication is successful, then you are logged into the Citrix session.



### **Configuring Citrix NetScaler using Okta**

Okta provides Single Sign-On (SSO) capability using Remote Authentication Dial-In User Service (RADIUS) for Citrix Virtual Apps and Desktops. ThinOS supports Okta through the Citrix NetScaler Gateway 11.0 or later. The Okta RADIUS Agent is used for user authentication. The Okta RADIUS server agent assigns the user authentication to Okta using single-factor authentication (SFA) or multifactor authentication (MFA).

For more information about configuring Citrix NetScaler Gateway to use the Okta RADIUS Agent, see the Citrix NetScaler Gateway Radius Configuration Guide at help.okta.com.

#### (i) NOTE:

• On the ThinOS client, you need FQDN at the login window. If you do not use username@fqdn during login, you must set the following INI parameter:

```
pnliteserver=https://<fqdn of NS Server> CAGUserAsUPN=yes
```

After you enable this INI parameter, the domain must use the domain.com format in the login window.

Phone authentication by using Okta is supported only in US and Canada.

#### Limitation

ThinOS version 8.6 supports only Okta with NetScaler Radius mode.

### **Citrix Cloud services**

ThinOS supports Citrix Cloud services. It acts as a single management console to deploy applications or desktops on any virtual or cloud setup for a secure digital workspace. For more information about Citrix Cloud services, see the Citrix Cloud article at docs.citrix.com.

### Citrix icon refresh

Citrix applications can be refreshed by clicking **Refresh** from PNMenu.

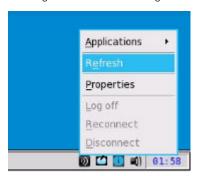
There are two methods to refresh the Citrix applications:

- · Manual refresh
- Auto refresh using the INI parameter

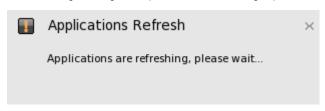
### **Refreshing Citrix applications manually**

To refresh the Citrix application manually, do the following:

1. For single StoreFront or PNAgent server, change the application in broker, and click Refresh from PNMenu.



The following message is displayed in the lower right pane during application refresh.

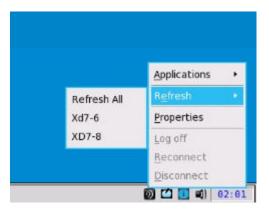


2. Applications are refreshed in Session bar list, Connect Manager list and App menu list.

The following log is displayed in the Event Log window:

ICA: refresh store "xxx"..." or "ICA: refresh PNAgent"xxx"...

3. For MultiFarm (StoreFront or PNAgent servers) or Multilogon (StoreFront or PNAgent servers), select a single server to refresh or click **Refresh All** to refresh all servers.



(i) NOTE:

Warning message is displayed when you open, edit, or remove applications when you refresh the applications.



4. Refresh scope covers the aspects such as, application removed, added, duplicated, disabled, enabled, icon/title change, and on/off desktop.

Active sessions that are started are not affected by application refresh.

The disconnect session can be reconnected after application refresh, if Automatic reconnection at logon is enabled in remote connection.

# Refreshing the Citrix applications automatically by using INI parameter

To automatically refresh the Citrix application, set the following INI parameter:

SessionConfig=ICA RefreshTimeOut=dd:hh:mm

For example, 01:01:22, means the application will start refresh automatically, every 1 day: 1 hour: 22 minutes.

#### **Limitations of Citrix icon refresh**

Following are the limitations of Citrix icon refresh:

- · Citrix icon refresh is supported in classic mode and storefront mode only.
- · Virtual Desktop Infrastructure (VDI) mode is not supported.

### Using multiple audio in Citrix session

ThinOS supports multiple audio device utilizations in the XenDesktop or XenApp version 7.6 and later. You can connect or disconnect the audio devices anytime during the session, but the behavior is similar to a local desktop. With multiple device support, you can connect multiple audio devices and select a specific device for a specific application.

The **Audio Plug N Play** policy must be enabled on the Citrix Remote Desktop Session (RDS) desktop. The **Audio Plug N Play** policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is enabled by default.

i NOTE: On the Citrix Virtual Desktop Infrastructure (VDI) desktop, pre-configuration is not required.

Supported devices—USB headset, webcam (without USB redirection), and analog headset devices are supported.

The following are valid working conditions for multiple audio:

- · Using Citrix HDX generic audio
  - 1. Select the audio device as PC Mic and Speaker.
  - 2. Configure the speaker or microphone.
  - 3. For secondary ringer, select the audio devices excluding the devices that are already selected.
- Using Citrix RealTime Multimedia Engine (RTME)
  - 1. Select the audio device as HID headset with PC Mic and Speaker.
  - 2. Set PC Mic and Speaker to configure the speaker or microphone.
  - 3. For secondary ringer, select the audio devices excluding the devices that are already selected.

The following scenarios must be considered during multiple audio settings:

- · ThinOS default audio is set to the latest plug-in audio device.
- · Session default audio is set to the ThinOS default audio. However, this option can be changed.
- · Restart Skype for Business/Lync client after you plug in and remove the device.
- · ICA RTP audio is supported with multiple audio connections.
- · During a call, the audio device settings can be switched without plugging in or plugging out the device.
- · Multiple audio can be shared across sessions.

#### Limitations

- · Wyse 3010 thin client with ThinOS and Wyse 3020 thin client with ThinOS are not supported.
- · In Wyse 3030 LT thin client with ThinOS, set the DP audio as the default audio device to use DP audio in a session.

## **Configuring ICA connections**

To configure the ICA connections:

- From the desktop menu, click System Setup, and then click Remote Connections.
  The Remote Connections dialog box is displayed.
- 2. In the Broker Setup tab, from the drop-down list, select the Broker type as None.

- 3. Click ICA connection protocol, and click Configure.
  - The **Default ICA** dialog box is displayed.
  - NOTE: Default ICA is always used for direct connection to a published application and not for StoreFront or PNAgent.
- 4. Click the Connection tab.

To configure the ICA connections, do the following:

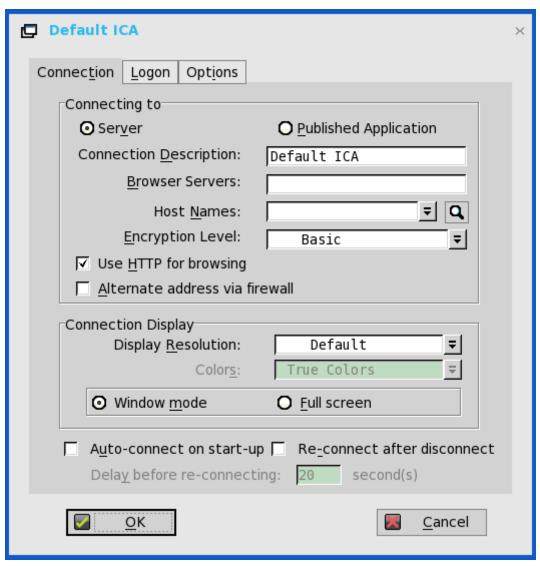


Figure 15. Default ICA

- a. Server or Published Application—Select the type of connection to which the settings apply.
- b. Connection Description—Enter the descriptive name that is to be displayed in the connection list (38 characters maximum).
- c. Browser Servers—Enter a delimited (comma or semicolon) list of IP addresses or DNS-registered names of ICA servers that contain the master browsers list, or that can direct to another server that contains the list.

The master browsers list is generated automatically by a browsing program on one of the ICA servers (selected by negotiation between servers). It is used to provide the information that is displayed in the Server Name or IP box. No entry is needed if the list is on an ICA server in the same network segment as the thin client. No entry is necessary if the connection is to a server, or if the server name or IP contains the IP address of the server.

d. Host Name or Application Name (title depends on the Server or Published Application option that is selected)—You can enter a delimited semicolon or comma-separated list of server host names or IP addresses, or you can select from the list of ICA servers or published applications that are obtained from the ICA master browser. You can also use **Browse** next to the box to make the selection you want.

If you enter a delimited list of servers, the thin client will attempt to connect to the next server on the list if the previous server attempt fails. If you use the list and the selected connection fails, the thin client will attempt to connect to the next one on the list.

- NOTE: The Host Name may be resolved using one of three mechanisms: ICA master browser, DNS, or WINS.

  Master browser is the only mechanism that can resolve a published application unless manual entry is made in DNS for the application. DNS uses the default domain name in the network control panel to attempt to construct an FQDN. However, it tries to resolve the name without using the default value.
- e. Encryption Level—Allows you to select the security level of communications between the thin client and the ICA server.
   Basic (the default option) is the lowest level of security. Basic enables faster communication between the device and the ICA server because it requires less processing than the higher levels of encryption.
  - NOTE: The encryption selection applies to the security of communications between the thin client and the ICA server only. It is independent of the security settings of individual applications on the ICA server. For example, most web financial transactions require the thin client to use 128-bit encryption. However, transaction information could be exposed to a lower level of security if the thin client encryption is not also set to 128-bits.
- f. Use HTTP for browsing—When selected, the thin client, by default, uses HTTP when browsing.
- g. Alternate address via firewall—When selected, the thin client uses an alternate IP address that is returned from the ICA master browser to get through firewall. This is used for the Windows login when the connection is activated.
- h. Display Resolution—Select the display resolution for this connection.
  - If you select the **Published Application** option, the Connection Display allows you to select the **Seamless Display Resolution** option.
- i. **Colors**—Select the color depth of the ICA session. If High Colors (16-bits) or True **Colors** is selected and the ICA server does not support this color depth, the thin client sets the color depth to the lower value, for example, 256 Colors (8-bits).
- j. Window mode and Full screen mode—Select the initial view of the application and desktop in a windowed screen or full screen.
- k. Auto-connect on start-up.—When this option is selected, the thin client automatically connects the session on start-up.
- I. Reconnect after disconnect—When this option is selected, the thin client automatically reconnects to a session after a non operator-initiated disconnect. The wait interval is the value that you set in the Delay before reconnecting box (enter the number of seconds 1–3600). The default is 20 seconds, if there is no INI parameter used for this connection, or if you are a stand-alone user.
- **5.** Click **logon** tab, and use the following guidelines:

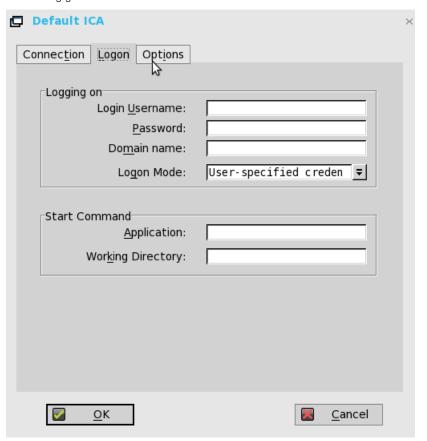


Figure 16. Default ICA—Logon

a. Logging on area—Enter username, password, domain name, and logon mode.

If the login username, password, and domain name boxes are not displayed, enter the information manually in the ICA server login screen.

- **Login Username**—Maximum of 31 characters is allowed.
- · Password—Maximum of 19 characters is allowed.
- **Domain Name**—Maximum of 31 characters is allowed.
- Logon Mode—Select User-specified credentials, Smart Card, or Local User.
- b. Start Command area—Server Connection Option Only—This area is disabled for a Published Application option.

**Application** (127 characters maximum) and **Working Directory** (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

**6.** Click the **Options** tab, and use the following guidelines:

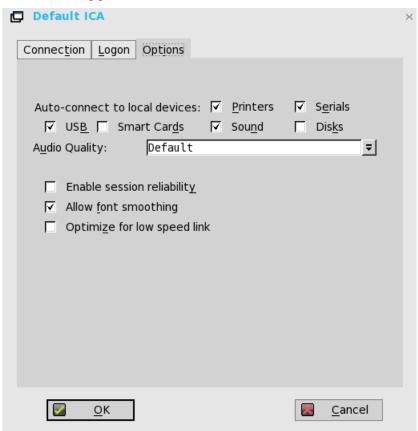


Figure 17. Default ICA—Options

- a. Autoconnect to local devices—Select any options (Printers, Serials, USB, Smart Cards, and Disks) to have the thin client automatically connect to the devices.
- b. Allow font smoothing—When selected, enables font smoothing (smooth type).
- c. Optimize for low speed link—When selected, allows optimization for low-speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dial-up.
- d. **Enable session reliability**—When enabled, session reliability allows you to momentarily lose connection to the server without having to re-authenticate upon regaining a connection. Instead of the connection time out, the session is kept alive on the server and is made available to the client upon regaining connectivity. Session reliability is most relevant for wireless devices.
- 7. Click **OK** to save the settings.

If the session reliability is enabled in an active session, and your network connection is not configured properly, a warning message is displayed with time elapsed after warning issuance.



Figure 18. Warning

# Support for multi-monitors in Citrix session

This section is applicable to Wyse 5070 thin client. ThinOS supports ICA desktop multiple monitors in XenDesktop/XenApp 7.6 and later versions.

#### Prerequisites:

- Increase the value of **MaxVideoMemoryBytes** REG\_DWORD to support one or more 4K resolution monitors. For more information, see Citrix documentation at support.citrix.com.
- Increase the display memory limit to support more color depth and higher resolution. For more information, see Citrix documentation citrix.com.

#### User scenario:

- 1. Connect multiple monitors to ThinOS device.
- 2. In the Display Setup dialog box, disable Mirror Mode, and configure the display layout.
- 3. Launch an ICA desktop with full screen.

#### Table 17. Display details

Platforms	Best Display resolution	Maximum number of system displays		
		Standard or RDS desktop— Windows 10 /2012 R2/ 2016	HDX 3D Pro desktop— Windows 10 with GRID K1/K2 GPU	
Wyse 5070 Extended thin client	1920 x 1080	6	4	
	2560 x 1440	6	4	
	3840 x 2160	6	Not supported, due to GRID K1/K2 vGPU profile limitation.	
Wyse 5070 thin client—	1920 x 1080	3	3	
Pentium processor	2560 x 1440	3	3	
	3840 x 2160	3	Not supported, due to GRID K1/K2 vGPU profile limitation.	
Wyse 5070 thin client—Celeron	1920 x 1080	2	2	
processor	2560 x 1440	2	2	
	3840 x 2160	2	Not supported, due to GRID K1/K2 vGPU profile limitation.	

#### Limitations

- For standard or RDS desktop (Windows10/2012 R2/2016) on Wyse 5070 Extended thin client, Dell recommends that you use up to four 4K monitors and remaining monitors with 1920 x 1080 resolution.
- For HDX 3D Pro desktop using vGPU or GPU Passthrough, the supported resolution and number of supported monitors is based on the NVIDIA's GRID support matrix.
- NOTE: For more information about the Citrix official multiple monitors support, see Citrix documentation at support.citrix.com.

### ICA Self Service Password Reset

You can do reset the password or unlock the account after you complete the security questions enrollment.

#### **Supported Environment**

- · Citrix Virtual Apps and Desktops 7.11 and later versions
- · Support Storefront server 3.7 and later versions
- · Self-Service Password Reset server 1.0 and later versions

#### Supported platforms—All platforms are supported

#### Limitations

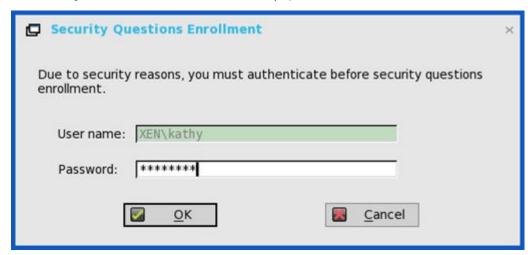
- · Supports only storefront server.
- The Legacy Account Self-Service (which needs Account Self-Service Server configured in ThinOS Remote Connections) is independent with this storefront version. Storefront version will cover Legacy Account Self-Service.
- · The security question enrollment is not supported in Virtual Desktop Infrastructure (VDI) mode.

### Before resetting password or Unlocking account

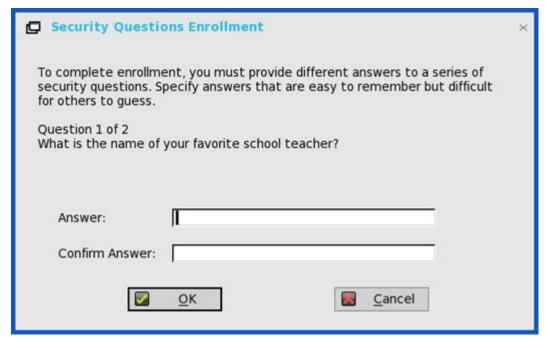
Before resetting your password or unlocking your account, you must register for the security questions enrollment. To register your answers for the security questions, do the following:

1. From the PNMenu, click the **Manage Security Questions** option (Classic and StoreFront only).

The Security Questions Enrollment window is displayed.



2. Enter the appropriate answers to the question set.





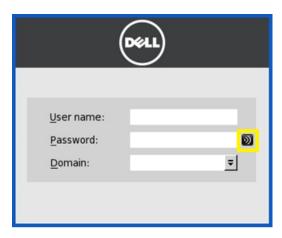
3. Click **OK** to register the security questions.



### **Using Account Self-Service**

After the security questions enrollment is complete, when ThinOS is connected to a StoreFront server with Self-Service Password Reset enabled, the **Account Self-Service** icon is displayed in the sign-on window.

- NOTE: If you enter wrong password more than four times in the Sign-on window, the client automatically enters the unlock account process.
- 1. Click the **Account Self-Service** icon to unlock your account or reset your password.



- i NOTE: You need to register the security questions for the users before using unlock account or reset password.
- 2. Click Unlock account or Reset password based on your choice, and then click OK.

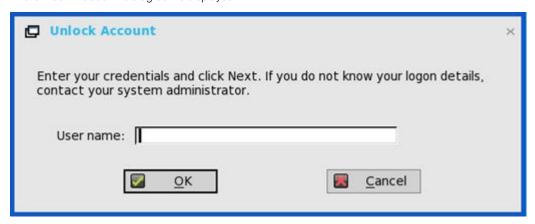


### **Unlocking account**

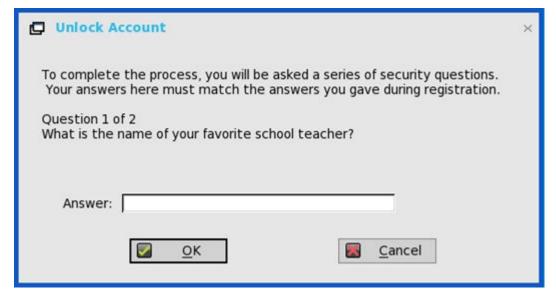
After you register the security questions, do the following to unlock your account:

- 1. Choose a task (Unlock account) in **Account Self-Service** window.
- 2. Enter the user name.

The **Unlock Account** dialog box is displayed.



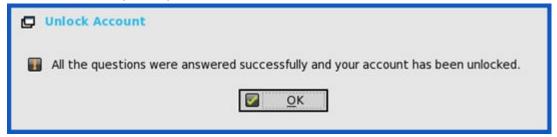
 ${\bf 3.}\;\;$  Enter the registered answers to the security questions.





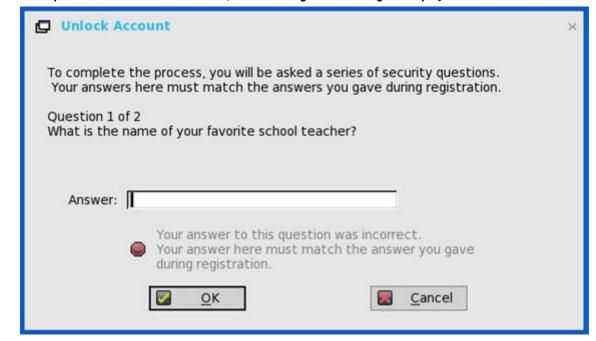
If the provided answers match the registered answers, then the Unlock Account dialog box is displayed.

4. Click **OK** to successfully unlock your account.



i NOTE:

• If the provided answers are incorrect, the following error message is displayed.



• If you provide the wrong answers more than three times, you cannot unlock the account or reset the password, and the following error messages are displayed.

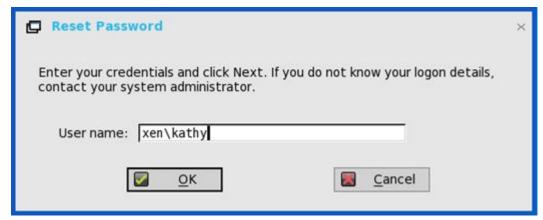


#### Resetting password

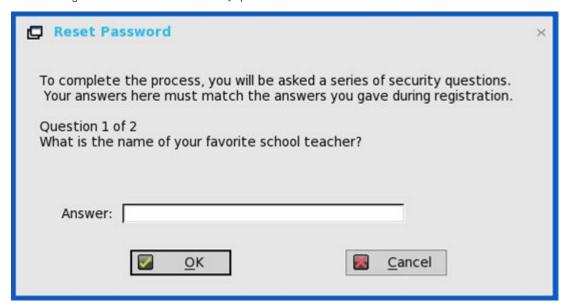
After you register the security questions, do the following to reset your password:

- 1. Choose a task (Reset password) in **Account Self-Service** window.
- 2. Enter the user name.

The **Reset Password** dialog box is displayed.



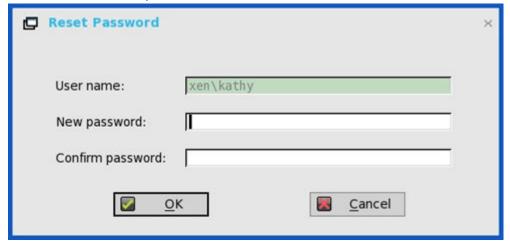
**3.** Enter the registered answers to the security questions.



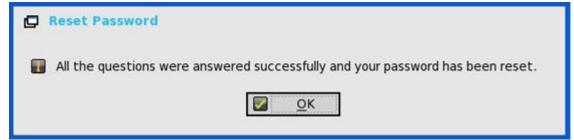


If the provided answers match the registered answers, then the  ${f Reset\ Password}$  dialog box is displayed.

4. Enter and confirm the new password.



5. Click **OK** to successfully change the password.



If you provide the wrong answers, you cannot reset the password, and an error message is displayed.

# **QUMU or ICA Multimedia URL Redirection**

QUMU utilizes ICA Multimedia URL Redirection. You are required to install a browser plug-in for this feature to work.

In earlier ThinOS releases, ICA Multimedia URL Redirection was partially supported. From ThinOS 8.4 release, a few enhancements are made to ICA multimedia URL redirection for better performance.

#### Supported protocols:

- · RTPS HLS
- · HTTP

**Verifying QUMU Multimedia URL Redirection**: While the video is playing, a noticeable lag or jump in the video window is observed when you move the browser on the screen or scroll the browser. This behavior indicates that the video is being redirected.

## **HTML5 Video Redirection**

HTML5 Video Redirection controls and optimizes the way XenApp and XenDesktop servers deliver HTML5 multimedia web content to users. From XenApp and XenDesktop 7.12, this feature is available for internal web pages only. It requires the addition of JavaScript to the web pages where the HTML5 multimedia content is available, for example, videos on an internal training site.

The following server policies must be enabled:

- · Windows Media redirection—By default this option is enabled.
- · HTML5 video redirection—By default this option is disabled.

**Verifying HTML5 Video Redirection**—While the video is playing, a noticeable lag or jump in the video window is observed when you move the browser on the screen or scroll the browser. This behavior indicates that the video is being redirected.

ThinOS event log for RAVE MMR is also displayed.

Sometimes, the initial playback does not work. After several seconds, the video is refreshed automatically, and you need to click playback from start again. During this time, the video will redirect.

#### Reference documents

- · Citrix sample video—www.citrix.com/virtualization/hdx/html5-redirect.html.
- ICA Multimedia policy settings—www.docs.citrix.com/en-us/xenapp-and-xendesktop/7-12/policies/reference/ica-policy-settings/multimedia-policy-settings.html.

# ICA SuperCodec

ICA SuperCodec is a H.264 decoder integrated on ThinOS ICA client side. Server encodes the session image into H.264 stream and sends it to client side. Client decodes the H.264 stream by SuperCodec and display the image on screen. This feature improves user experience especially for HDX 3D Pro desktops.

#### **Supported Environment**

Citrix Virtual Apps and Desktops (formerly XenDesktop) and Citrix Virtual Apps (formerly XenApp) version 7.5 or later versions

#### **Prerequisities**

In Citrix Virtual Apps and Desktops (formerly XenDesktop) and Citrix Virtual Apps (formerly XenApp) version 7.9 and later, the default setting for **Use video codec for compression** is **Use when preferred**. For best performance on ThinOS device, Dell recommends that you set the **Use video codec for compression** policy to **For the entire screen**. Alternatively, you can also set the policy to **Do not use video codec**. This allows ThinOS to use **ThinWire Plus** that saves bandwidth and reduces CPU overhead.

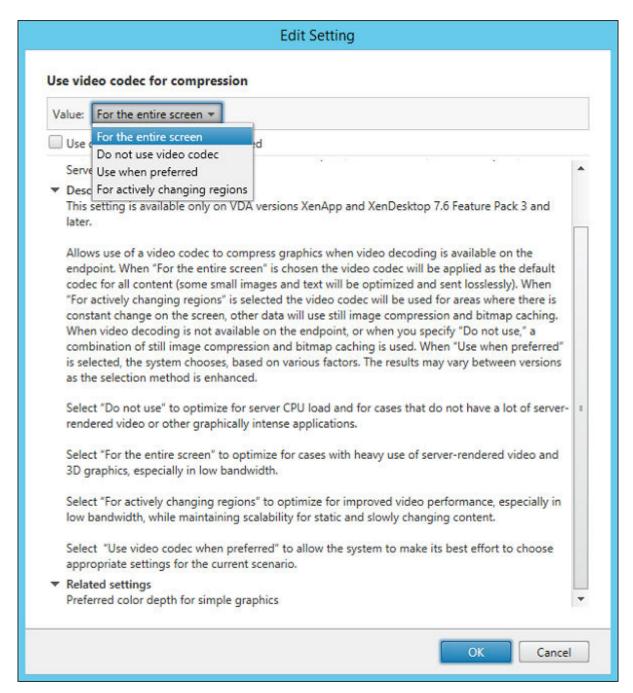


Figure 19. Use video codec for compression setting

- ThinWire Plus—Equivalent to Do not use video codec option
- Fullscreen H.264—Equivalent to For the entire screen option
- · Selective H.264—Equivalent to For actively changing regions

#### Verifying the working status of the ICA connections

• For Dell Wyse 3010, 3020 and 3040 thin clients—By default, ICA SuperCodec is enabled when the ThinOS display resolution is lesser than or equal to 1920 x 1080. If display resolution is higher than 1920 x 1080, the following ThinOS event log is displayed:

```
System resolution exceeds hardware limitation (1920 x 1080), disable SuperCodec
```

**For Dell Wyse 3040 thin client**—By default, ICA SuperCodec is enabled when the ThinOS display resolution is lesser than or equal to 1920 x 1200. If ThinOS resolution is higher than 1920 x 1200, the following ThinOS event log is displayed:

System resolution exceeds hardware limitation (1920 x 1200), disable SuperCodec

• For Dell Wyse 5040, 5060, 5070 thin clients—ICA SuperCodec is always enabled without any limitation. The following ThinOS event log is displayed:

ICA: SuperCodec enabled

NOTE: For ICA connections, there is no INI parameter.

If you set the Use video codec for compression policy to Do not use video codec, ICA SuperCodec is disabled, and ThinOS does not print any log.

## **Anonymous logon**

Anonymous logon feature enables the users to log into the StoreFront server configured with unauthenticated store without Active Directory (AD) user credentials. It allows unauthenticated users to access the applications instead of AD accounts.

i NOTE: Anonymous logon is not supported with legacy mode of StoreFront server.

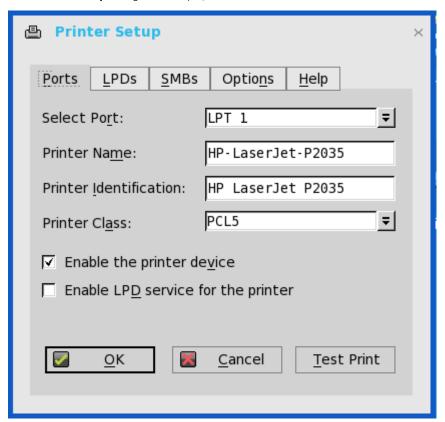
# Configuring the Citrix UPD printer

Use of Citrix Universal Printer Driver (Citrix UPD) ensures that all printers connected to a client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center. Citrix UPD is the base of Citrix Universal Printer. It is an auto-created printer object that uses the Citrix UPD and is not tied to any specific printer defined on the client.

To configure the Citrix UPD usage on ThinOS:

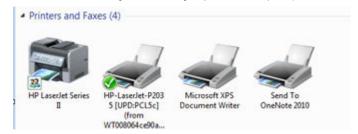
- 1. Connect a printer to ThinOS client.
- 2. From the desktop menu, click **System Setup**, and then click **Printer**.

The **Printer Setup** dialog box is displayed.



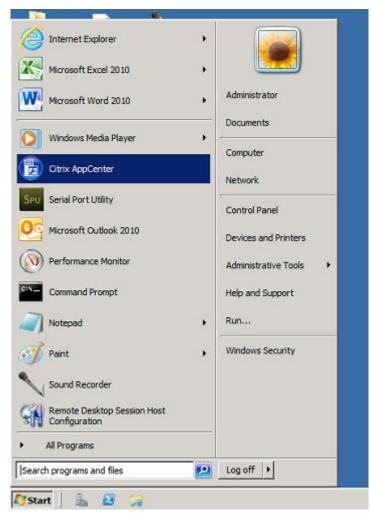
- **3.** Enter the name of the printer in the **Printer Name** box.
- **4.** Enter any string of the Printer identification in the **Printer Identification** box.
- 5. Select the type of the printer class from the drop-down list, select the check box to enable the **printer device** and then click **OK**.
- 6. Start a Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) or Citrix Virtual Apps (formerly Citrix XenApp) application connection.

7. Open the Devices and Printers in the desktop or application, notice the printer is mapped as UPD printer by default. You can use the HP-LaserJet-P2035 [UPD:PCL5c] to perform the print job.

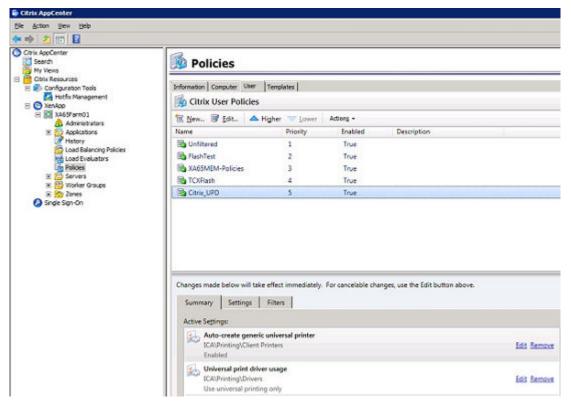


#### Citrix UPD configuration on server

- **a.** To enable the printer policy, use the following guidelines:
  - i. To enable the printer policy in Citrix Virtual Apps 6.5– Go to the DDC Server, click **Start** > **Citrix AppCenter** .



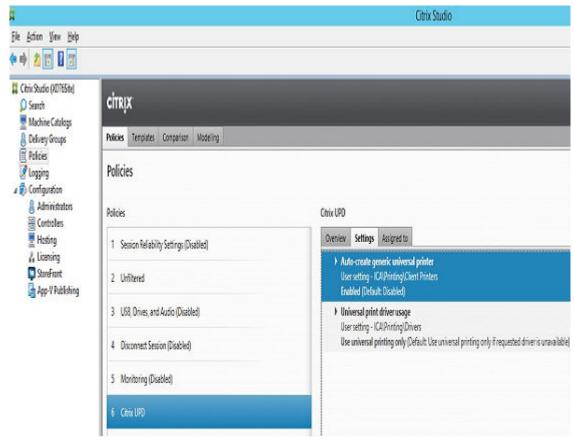
- ii. Click Citrix Resources > XenApp > Policies > User > Settings > Printing > Client Printers and enable the Auto-create generic universal printer.
- iii. Click **Printing > Drivers** and set the **Universal print driver usage** to **Use universal printing only** from the drop-down menu available.



- iv. To enable the printer policy in Citrix Virtual Apps and Desktops 7.5 and later versions, do the following:
  - i. Go to the Citrix DDC server,

Ordered Listribustbelio > policies and add a policy. Enable the Auto-create generic universal printer option.

Ordered his Universal print driver usage to Use universal printing only from the drop-down menu.



b. Check registry and make sure the same driver has been installed.

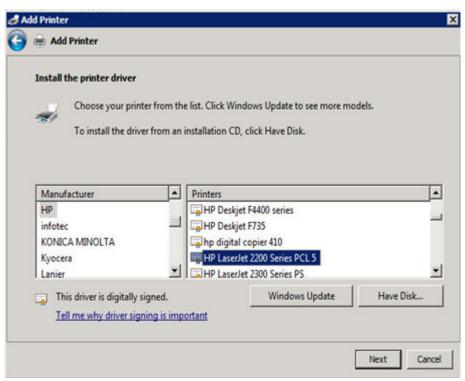
- i. Check the drivers in registry of the server or desktop which you want to connect. The server or desktop must have ps, pcl5, pcl4 drivers in the registry and the same driver must be installed on the server or desktop.
- ii. Go to HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\. ThinOS does not support EMF and XPS
  - NOTE: The supported drivers in the following table are one of the supported drivers for Citrix UPD used in ThinOS. One of the recommended driver is provided here as an example.

The supported drivers are listed in the following table:

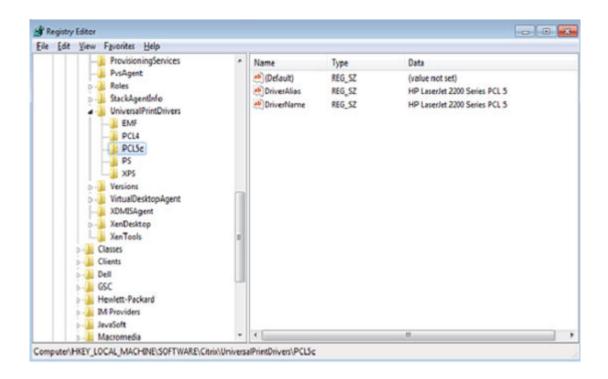
Table 18. Supported drivers

Printer class	Printer driver				
PS	HP Color LaserJet 2800 Series PS				
PCL5	HP LaserJet 2200 Series PCL 5				
PCL4	HP LaserJet Series II				

- c. If the server or desktop which you want to connect does not have these drivers, follow the steps mentioned here:
  - i. For example, in Citrix Virtual Apps 6.5 for Windows Server 2008 R2, add PCL driver in Server. Go to **Device and Printers** > **Select any printer** > **Click Printer server properties** > **Driver tab** and then add **HP LaserJet 2200 Series PCL 5 driver**.



ii. Under HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\PCL5c\, change DriverAlias and DriverName HP LaserJet 2200 Series PCL 5.



### Flash Redirection

The Flash Redirection solution is to off-load flash content to the ThinOS client, and locally render and decode the flash playback. The off-loading is conducted by Citrix HDX Flash Redirection. The local rendering and decoding process are conducted by customized flash player and other multimedia process that runs locally on ThinOS.

**Supported Environment**— Supports only Citrix Connections with XenApp 6.5 and later versions and XenDesktop 7.0 and later versions.

#### Supported Platforms:

- Wyse 3030 LT with ThinOS
- · Wyse 3030 LT with PCoIP
- Wyse 3040 with ThinOS
- Wvse 3040 with PCoIP
- Wyse 5010 with ThinOS (D10D)
- Wyse 5010 with PCoIP (D10DP)
- · Wyse 5040 AIO thin client (5212)
- · Wyse 5040 AIO with PCoIP (5213)
- Wyse 5060 with ThinOS
- Wyse 5060 with PCoIP
- Wyse 7010 with ThinOS (Z10D)

#### Flash Redirection

#### Required packages

User must install the FR.i386.pkg package for the feature to work:

#### Installation of packages

To install the required packages, follow the steps mentioned here:

- 1. Upload packages to directory \wnos\pkg\.
- 2. Ensure that the INI autoload is not set to 0. Set INI AutoLoad=1 AddPkg=FR in wnos.ini.
- 3. Restart the client to read the file server and wait till the auto installation of packages is complete. You can view the installed packages in the **Packages** tab in the **System Tools** dialog box.
- 4. Server configuration for Flash redirection

**a.** To ignore the differences in flash player versions, user must add the FlashPlayerVersionComparisonMask and ClientFlashPlayerVersionMinimum registry key on the desktop.

If it is Citrix Virtual Apps 6.5, IEBrowserMaximumMajorVersion registry key is required to ignore the differences in IE Browser versions.

For more information, see docs.citrix.com/en-us/xenapp-and-xendesktop/7-9/hdx/flash-redirection.html.

From Citrix Virtual Apps and Desktops 7.9, you must add more entries in registry for HDX FR to work. For information about these additional entries, refer to Citrix Technical documents.

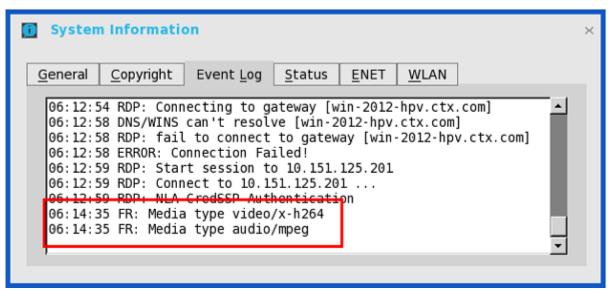
#### 5. Client configuration for Flash redirection

By default, no client configuration is required. New INI parameters are added to support HDX FR Client configurations, for example, to fetch the server side content. The newly added INI parameters are:

```
SessionConfig=ICA\
HDXFlashUseFlashRemoting=Never | Always (default) \
HDXFlashEnableServerSideContentFetching=Disabled (default) | Enabled \
```

#### How to verify it is working or not working

- **a.** Right-click the flash video to know the flash player version. It displays version information of the customized player at ThinOS client side which is 11.1.102.59. If the flash player version is different, then it is unsuccessful server rendering.
- b. During the flash playback, it will display ThinOS event logs for HDX FR in the System Information dialog box.
  - i. FR: Media type video/x-264
  - ii. FR: Media type audio/mpeg



For information about basic operations on Citrix HDX flash redirection and policies configurations, see Citrix documentation.

#### **Known Issues**

- a. Playback flash videos in Internet Explorer browser with normal security settings.
- **b.** Playback with videos ≤ 720p; the 1080p video may show graphic issue.
- c. Playback full screen video with resolution ≤ 1920 x 1200. For example, full screen playback with ThinOS resolution 1920 x 1200; in 2560 x 1600 full screen video there could be graphic issues.
- d. After flash video is loaded, the video content remains in the initial size. For example, resizing browser does not resize the video content.
- e. Only English font is supported. For example, subtitles in other languages are not properly displayed.
- f. Playback YouTube.com videos may run into some issues. For example, cannot show video unless you copy the URL and paste it to the browser.

Limitation—Non-Latin URLs are not supported.

# **Configuring VMware**

VMware virtualization enables you to run multiple virtual machines on a single physical machine. VMware Horizon Client is a locally installed software application that communicates between View Connection Server and thin client operating system. It provides access to centrally hosted virtual desktops from your thin clients.

In every ThinOS release, the Horizon Client version may be updated to newer version. For information about the latest Horizon Client version, see the latest *Dell Wyse ThinOS Release Notes* at www.dell.com/manuals.

NOTE: If you are upgrading your thin client to the latest ThinOS version, you must ensure that the Horizon server or agent version is updated to support the latest horizon client version. For more information about the client and server/agent version compatibility, see the VMware Product Interoperability Matrices page at www.vmware.com.

This section provides information about how to configure a VMware broker connection on your ThinOS device, and other VMware features that you can configure on ThinOS.

# Configuring the VMware broker connection

To configure the VMware broker setup:

- From the desktop menu, click System Setup, and then click Remote Connections.
   The Remote Connections dialog box is displayed.
- 2. In the Broker Setup tab, from the drop-down list, select VMware view, and do the following:
  - **Broker Server**—Enter the IP address/Hostname/FQDN of the Broker Server.
  - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semicolon, and is case-sensitive.
  - **Security mode**—Select the preferred security mode from the following options:
    - Warning—Warn Security requires FQDN address with self-signed certificate, or without any certificate, but corresponding
      warning message is displayed for user to continue.
    - Full—Full Security requires FQDN address with domain certificate.
    - Low—Security allows FQDN/IP address with/without certificate.
    - o **Default**—Follows global security mode settings.
  - Connection Protocol
     —From the drop-down list, select the type of protocol connection. By default, the option is set to Server
     Default.
    - NOTE: The PCoIP only connection protocol is applicable only to PCoIP clients. If you do not install Horizon package, then the Blast only protocol option is not available for selection. PCoIP protocol is required for PCoIP session. Horizon package is required for Blast session.

The available options are:

- Server default—Select this protocol connection to display the desktop with default protocol as configured in the VMware View Admin console, for each pool in the broker. If a desktop pool is configured with default protocol as RDP in the View Admin console, then only the RDP connection of the desktop is displayed in ThinOS after users sign in to the device.
- All Supported—Select this protocol connection to display the desktop in all the available connections, when a desktop pool is
  configured to allow users to select protocol as yes. If a desktop is configured with default protocol as PCoIP and allow user to
  select protocol as no, then ThinOS only displays the desktop in the PCoIP connection.
- RDP only—Select this protocol connection to display the desktop in RDP connection only. If a desktop pool is configured with default protocol as PCoIP in the View Admin console, and allow user to select protocol as no, then this desktop is not displayed in ThinOS after user signs in to the device.
- PCoIP only—This option is available only for PCoIP enabled clients. Select this protocol connection to display only the
  desktop in the PCoIP connection, for each pool in the broker. If a desktop pool is configured with default protocol as RDP in
  the View Admin console, and allow user to select protocol as no, then this desktop is not displayed in ThinOS after user signs in
  to the device.
- Blast only—VMware Blast display protocol can be used for remote applications and for remote desktops that use virtual
  machines or shared-session desktops on an RDS host. Select this protocol connection to display the desktop with the Blast
  protocol.
- Blast and RDP—This option is available on both PCoIP enabled clients and non-PCoIP clients. Select this protocol connection
  to display the desktop in either Blast or RDP connections.
- Blast and PCoIP—This option is available only for PCoIP enabled clients. Select this protocol connection to display the desktop in either Blast or PCoIP connections.

- PCoIP and RDP—This option is available only for PCoIP enabled clients. Select this protocol connection to display the desktop in either PCoIP or RDP connections.
- **Log in anonymously using Unauthenticated Access**—Select this check box to anonymously log in to the VMware session with application remoting.
- 3. Click **OK** to save the settings.

### **Limitations**

- ThinOS supports four displays with 4K resolution in a Horizon blast session. Due to low performance, Dell recommends that you do not
  use four displays with 4K resolution.
- · Vertical Synchronization does not work in Blast session with four 4K resolution.
- · Video performance is low when you play a video in Blast session with 4K resolution.
- ThinOS supports audio device USB redirection. However, Dell does not recommend using audio device USB direction due to low audio quality.
- · The text copy and paste functionality between local and Blast sessions works only after you perform a session switch.

### **VMware Horizon Client feature matrix**

Table 19. VMware Horizon Client feature matrix

	Client type	ThinOS			
Client Appearance and Workflow	Customer branding	Not supported			
	Kiosk mode	Supported			
	In-product help	Not supported			
	Online help	Not supported			
	English localization	Supported			
	French localization	Supported			
	German localization	Supported			
	Japanese localization	Supported			
	Traditional Chinese localization	Supported			
	Simplified Chinese localization	Supported			
	Korean localization	Not supported			
	Spanish localization	Not supported			
Broker Connectivity	XML-API version	13			
	SSL	Supported			
	SSL certificate verification	Supported			
	Disclaimer dialog	Supported			
	Security Server compatibility	Supported			
	UAG compatibility	Supported			
	Multi-broker/Multi-site redirection - DaaS	Not supported			
	Client info	Supported			
	Phonehome	Not supported			
Broker Authentication	Password authentication	Supported			
	Password change	Supported			
	RSA authentication	Supported			

Table 19. VMware Horizon Client feature matrix (continued)

	Client type	ThinOS			
	Radius	Supported			
	Integrated RSA SecurID token generator	Not supported			
	Single Sign On	Supported			
	Log in as current user	Not supported			
	Nested log in as current user	Not supported			
	Biometric authentication	Not supported			
	Unauthentication access	Supported			
Smart card	x.509 certificate authentication (Smart Card)	Supported			
	CAC support	Supported			
	.Net support	Supported			
	PIV support	Not supported			
	Java support	Not supported			
	Purebred derived credentials	Not supported			
Desktop Operations	Reset	Supported			
	Restart	Not supported			
	Log off	Supported			
Session Management (Blast Extreme and	Switch desktops	Supported			
PCoIP)	Multiple Connections	Supported			
	App Launch on Multiple end points	Supported			
	Auto-Retry	Supported			
	Auto-Retry 5+ minutes	Supported			
	Fullscreen mode	Supported			
	Fullscreen toolbar	Not supported			
	Windowed mode	Supported			
	Time Zone Synchronization	Supported			
	Jumplist integration (Windows 7-Windows 10)	Not supported			
Client Customization	Command Line Options	Not supported			
	URI Schema	Not supported			
	Preference File	Supports only Blast			
	Non Interactive Mode	Not supported			
	GPO-based customization	Not supported			
Protocols supported	Blast Extreme	Supported			
	H.264 - HW decode	Supported			
	H.265 - HW decode	Not supported			
	JPEG/PNG	Supported			

Table 19. VMware Horizon Client feature matrix (continued)

	Client type	ThinOS
	Blast Extreme Adaptive Transportation	Supported
	RDP 6.x	Supported
	RDP 7.x	Supported
	RDP 8.x, 10.x	Supported
	PCoIP	Supported
Protocol Enhancements Protocol	RDP-VC Bridge	Supports only Blast
Enhancements	Session Enhancement SDK	Not supported
Features / Extensions Monitors / Displays	Dynamic Display Resizing	Supported
	Multiple Monitor Support	Supported
	External Monitor Support	Supported
	Display Pivot	Supported
	Multiple Aspect Ratio support	Supported
	Number of displays supported	4
	4K resolution	3840×2160
	5K resolution—Supported only on Dell U49 series monitors	5120x1440
	Video out	Supported
	High DPI scaling	Not supported
	DPI Sync	Supported
	Exclusive Mode	Not supported
	Multiple Monitor Selection	Supported
Input Device (Keyboard / Mouse)	Relative mouse	Supported
	External Mouse Support	Supported
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported
	Unicode Keyboard Support	Not supported
	International Keyboard Support	Supported
	Input Method local/remote switching	Not supported
	IME Sync	Not supported
Clipboard Services	Clipboard Text	Supports only Blast
	Clipboard Graphics	Not supported
	Clipboard memory size configuration	Not supported
	Drag and Drop	Not supported
Client Caching	View Agent to Client-side caching	Supports only Blast
Connection Management	Blast network recovery	Supported
	IPv6 support	Supported
	PCoIP IP roaming	Supported

Table 19. VMware Horizon Client feature matrix (continued)

	Client type	ThinOS			
High-Level Device Redirection	Serial (COM) Port Redirection	Not supported			
	Client Drive Redirection/File Transfer	Not supported			
	Scanner (TWAIN/WIA) Redirection	Not supported			
	x.509 Certificate (Smart Card)	Supported			
	Gyro Sensor Redirection	Not supported			
Real-Time Audio-Video	Analog in (input)	Supported			
	Real-Time Audio-Video	Supported			
	Multiple webcams	Not supported			
USB Redirection	Generic USB/HID	Supported			
	Policy: ConnectUSBOnInsert	Supported			
	Policy: ConnectUSBOnStartup	Supported			
	Connect/Disconnect UI	Not supported			
	USB device filtering (client side)	Supported			
	Isochronous Device Support	Supported			
	Split device support	Supported			
	Bloomberg Keyboard compatibility	Supported			
	Smartphone sync	Supported			
	USB 3.0	Supported			
	USB Redirection USB storage devices	Supported			
Unified Communications	Cisco UC Jabber	Not supported			
	Avaya UC One-X Desktop	Not supported			
	Mitel UCA	Not supported			
	Microsoft Lync 2013	Not supported			
	Skype for business	Supports only Blast			
Multimedia Support	Multimedia Redirection (MMR)	Not supported			
	Flash URL Redirection (Unicast/Multicast)	Not supported			
	Flash Redirection	Not supported			
	HTML5 Redirection	Not supported			
Graphics	vDGA	Supported			
	vSGA	Supported			
	NVIDIA GRID VGPU	Supported			
	Intel vDGA	Supported			
	AMD vGPU	Supported			
Mobile Support	Client-side soft keyboard	Not supported			
	Client-side soft touchpad	Not supported			
	Full Screen Trackpad	Not supported			

Table 19. VMware Horizon Client feature matrix (continued)

	Client type	ThinOS				
	Gesture Support	Not supported				
	Multi-touch Redirection	Not supported				
	Presentation Mode	Not supported				
	Unity Touch	Not supported				
Printing	Printer Redirection	Supports only Blast				
	Location Based Printing	Supports only Blast				
	Native Driver Support	Not supported				
	PDF Download	Not supported				
Security	FIPS-140-2 Mode Support	Not supported				
	Imprivata Integration	Supported				
	TLS 1.0	Supported				
	TLS 1.1	Supported				
	TLS 1.2	Supported				
	Client Device Authentication	Not supported				
Session Collaboration	Session Collaboration	Not supported				
	Read-only Collaboration	Not supported				
Update	Automatic Updates	Not supported				
	App Store update	Not supported				
Other	Smart Policies	Not supported				
	File Type Association	Not supported				
	URL content redirection	Not supported				
	Remember credentials	Supported				
	Access to Linux Desktop - Blast Protocol	Supported				
	Audio Playback	Supported				
	Seamless Window	Not supported				
	Launching multiple client instances using URI	Not supported				
	One-click Install of Client	Not supported				
	Parameter pass-through to RDSH apps	Not supported				
	Performance Tracker	Supported				
	Shortcuts from server	Not supported				
	Workspace ONE mode	Not supported				

 $\textbf{Supported} \\ - \\ \textbf{Both PCoIP and Blast protocols are supported}.$ 

**Not supported**—Both PCoIP and Blast protocols are not supported.

# Using VMware Horizon View broker and desktop

**VMware Horizon View Broker timeout**—The VMware Horizon View Broker timeout does not force the user to sign out from the broker anymore when the secure tunnel is enabled.

In earlier version of ThinOS, when the broker times out, the user session is disconnected and the user is logged out from the broker. From ThinOS 8.2 release, ThinOS disconnects the user session from the broker, but does not force user logout. This is because the user has local connections other than the broker desktop, and these connections are active when the broker timeout is reached.

**PCoIP session NUM/CAP keyboard status synchronizes with session instead of thin client**—This is applicable for session startup only. The PCoIP session keyboard NUM/ CAP status synchronizes from remote session to client, whereas RDP/ ICA synchronizes status from local to remote session.

#### For example:

- 1. Set keyboard NUM=off in current PCoIP session.
- 2. Disconnect the session.
- 3. Set client keyboard NUM=on.
- 4. Reconnect to the PCoIP session.
- 5. The keyboard NUM status in both session and client is updated to NUM=off.

**RDS desktop through PCoIP/Blast**—You can view and connect to the Remote Desktop Service (RDS) desktop through the PCoIP/Blast protocol in the broker using PCoIP/Blast enabled the ThinOS clients. In VMware Horizon View 6.0 and later versions, the RDS desktop has RDP, PCoIP, or Blast connections based on server configurations.

i NOTE: The Horizon application is supported on both PCoIP and Blast. RDP is not supported.

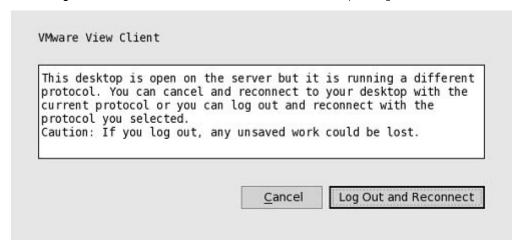
The RDS desktop protocol switch message dialog box is provided in this release. A typical user scenario is as follows:

- 1. Connect to the RDS desktop through protocol. For example, RDP.
- 2. Disconnect from the desktop.
- 3. Connect to the same RDS desktop through another protocol. For example, PCoIP.

The message dialog box is displayed, allowing you with an option to continue.

The options available are:

- · Cancel—You can end the PCoIP connection, and connect to the desktop in RDP again.
- · Log Out and Reconnect—You can connect to the desktop through PCoIP, and the earlier session in RDP is logged out.



USB redirection RDS desktop through PCoIP/Blast—This feature is supported.

**USB audio redirection**—USB audio redirection enables you to use USB audio devices in the remote session. However, Dell does not recommend that you enable the USB audio redirection because of sound quality.

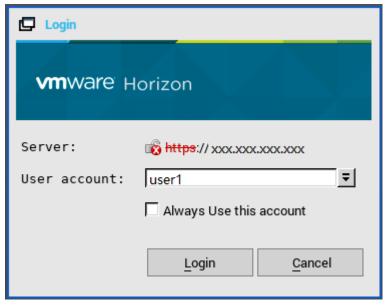
Using unauthenticated access—You can anonymously log in to the VMware session with application remoting.

To use the unauthenticated option, do the following:

- 1. On your AD server, create two anonymous users, for example, anonymous1 and anonymous2.
- 2. Log in to your View Admin web portal.
- Navigate to Users and Groups > Unauthenticated Access, and add the two new anonymous users to the View Connection Manager.

- 4. Navigate to View Configurations > Select Servers > Connection Servers, and select your connection server.
- 5. Click Edit > Authentication tab, and select the Enabled for unauthenticated access check box. Do not select any users for the default unauthenticated user.
- 6. Go to **Application Pools**, add a few applications that you have installed on the Virtual Machine, and entitle the applications to anonymous1 and anonymous2 user.
- 7. On the ThinOS broker setup dialog box for VMware View, select the Log in anonymously using Unauthenticated Access check box.
- 8. Restart your thin client.

The following dialog box is displayed:



9. Select the **Always use this account** check box to use the login account that you have specified. You cannot change this login account for other users.

**Hide Server URL**—The server URL can be hidden in the Horizon View broker UI. You can configure this setting using any of the following methods:

- · Using View Connection Server web portal
  - 1. Log into your View Connection Server web portal.
  - 2. Navigate to View Configuration > Global Settings > Edit, select the Hide server information in client user interface check box, and clear the Hide domain list in client user interface check box.
  - 3. Click OK.
  - 4. Log in to the VMware Horizon broker.

The server URL is hidden, and the domain list is displayed.

· Using INI parameter

Use the INI parameter, ConnectionBroker=vmware DisableShowServer=yes.

Hide Domain List—The domain list can be hidden in the Horizon View Broker logon UI. To configure this setting, do the following:

- 1. Log in to your View Connection Server web portal.
- 2. Navigate to View Configuration > Global Settings > Edit, select the Hide domain list in client user interface check box, and clear the Hide server information in client user interface check box.
- 3. Click OK.
- 4. Log in to the VMware Horizon broker.

The domain list is hidden, and the server URL is displayed.

# Enable username hint for smart card login

You can enable users to specify the account to be used in the **Username hint** field when you log in to a Horizon View session using a smart card. Enabling this option allows you to use a single smart card certificate to authenticate to multiple user accounts.

To enable the username hint field, do the following:

- 1. Log in to the View Administrator Admin console, and click View Configuration > Servers.
- 2. On the Connection Servers tab, select the View Connection Server instance, and click Edit. The Edit Connection Server settings page is displayed.
- 3. Click the Authentication tab.
- 4. In the View Authentication section, select the Allow smart card user hints check box.

You cannot configure the smart card user name hints feature when you set the smart card authentication to Not Allowed.

5. Click OK.

On the ThinOS client, log in to a Horizon View session with a smart card. In the VMware Horizon View broker sign-on window, enter the username and the smart card PIN to authenticate the user.

NOTE: If the user name does not match the smart card certificate user, an error message No user could be found for your Certificate is displayed.

# **Supporting VMware Real Time Audio-Video**

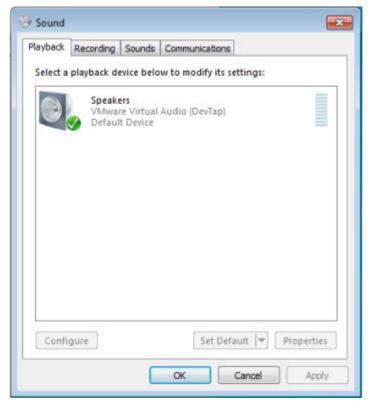
Use the Real-Time Audio-Video feature to run Skype and other online conference applications on the remote desktop. Using this feature, both audio and video devices that are connected to your thin client are available to use for VoIP in remote desktop.

To know more about the VMware Real Time Audio-Video support, go to pubs.vmware.com/horizon-62-view/topic/com.vmware.horizon-view.desktops.doc/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html.

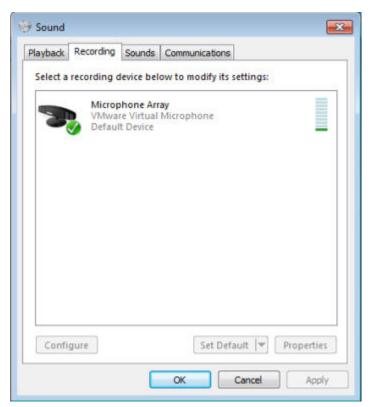
NOTE: There is no additional configuration for ThinOS. RTAV video requires RTME package to be installed on your device.

To validate the VMware Real Time Audio-Video, do the following:

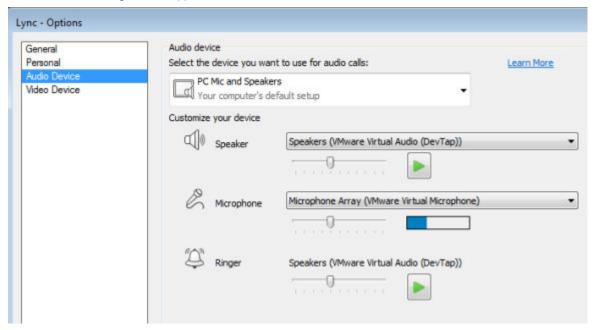
- 1. Connect to the VMware PCoIP or Blast desktop with the audio and video devices.
  - i NOTE: USB redirection must be disabled for the audio/video devices.
- 2. Verify the audio playback of the system using the VMware virtual audio.



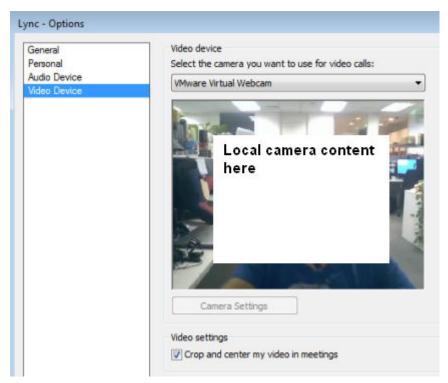
**3.** Verify the system audio recording using the VMware virtual microphone.



4. Verify the audio settings in VoIP application.



5. Verify the video settings in VoIP application using the VMware virtual webcam.



6. Start the audio or video calls.

#### Dependencies and known issues

- Dependency: RTME.i386.pkg needs to be installed for RTAV video.
- The answer call button of the local audio device, supported by HDX RTME, is not supported by RTAV.
- · RTAV does not support RDS desktop, for example, 2008 R2/ 2012 R2 according to VMware.
- · Support for PCoIP and Blast protocol only. RDP protocol is not supported according to VMware.
- Webcam preferences are not supported. For example, the first webcam displayed in the Camera tab in local peripheral settings is used always.
- Camera/Video: High Definition video is not supported because of the RTAV limitation. The local camera setting does not affect RTAV video because of the application design. Dell recommend users not to interfere with the local camera settings.

## **VMware Blast**

VMware Blast display protocol can be used for remote applications and for remote desktops that use virtual machines or shared-session desktops on an RDS host. Select this protocol connection to display the desktop with the Blast protocol.

NOTE: When you pause the pointer over the connection icons, the corresponding connection protocols are displayed in tooltip. This is designed for RDSH applications. From ThinOS 8.4 release, RDSH application is supported for both PCoIP and Blast protocol. These two protocols share the same application icon, and hence it is necessary for you to pause the pointer over the connection icons to identify its protocol.

#### Blast feature matrix on ThinOS

Table 20. Blast feature matrix

Blast features	Support on ThinOS	Comments/ Known issues				
H.264 offload	Yes	Blast H.264 is not supported on Wyse 5010 thin client, Wyse 5040 AIO thin client, and Wyse 7010 thin client.				
VDI desktops	Yes	N/A				
RDSH desktops	Yes	N/A				

Table 20. Blast feature matrix (continued)

Blast features	Support on ThinOS	Comments/ Known issues
RDSH applications	Yes	Application window does not support Seamless mode. For example, all applications open in single window because of the VMware limitation.
		RDSH application supports the PCoIP protocol from ThinOS 8.4, with same limitation.
Unified communication	No	Third-party plug-ins are not available.
Microsoft Lync VDI plug-in	No	N/A
Real-Time Audio-Video (RTAV)	Yes	N/A
Skype for Business	Yes	N/A
Windows Media MMR	No	N/A
Flash URL multicast	No	N/A
Printer redirect	Yes	Supports printer redirection, and printer mapping with virtual print.
Smartcard redirect	Yes	N/A
Scanner redirect	No	N/A
Serial port redirect	No	N/A
USB redirect—VDI/ RDSH	Yes	Enabled by default.
Client drive redirect	No	N/A
Linux desktop	Yes	N/A
Copy Paste text	Yes	See, VMware Horizon server and client configurations/documentation.
VPN connect	Yes	N/A
AES 128/256	Yes	See, ThinOS AES design.
Multi-display/ 4K/ 32-bit	Yes	See, VMware Blast support information. For example, the prerequisite is VM video RAM.
ClearType fonts support	No	ThinOS supports TrueType fonts.
3D display	Yes	See, VMware Blast support information.
Blast recovery from network interrupt	Yes	Requires Horizon View agent 7.0.1.

For more information about VMware Horizon Blast, see VMware documentation. For information about Blast Virtual Printing on ThinOS, see Blast Virtual Printing.

# VMware Horizon Virtualization Pack for Skype for **Business**

The VMware Horizon Virtualization Pack for Skype for Business enables you to use Skype for Business in a VMware Horizon desktop. Microsoft Skype for Business is a unified communications platform that delivers an optimized user experience for online messaging, audio, and video calling and so on.

ThinOS supports VMware Horizon Virtualization Pack for Skype for Business in a Blast session only. PCoIP and RDP protocols do not support this feature.

### Installing the horizon package on ThinOS

You must install the horizon.i386 package on ThinOS to use the VMware Blast protocol. For information about the latest version of the horizon package delivered in ThinOS version 8.6, see the Dell Wyse ThinOS version 8.6 Release Notes at www.dell.com/support.

To install the horizon package:

- Extract the horizon package.
- The horizon.i386.pkg files are unzipped to a valid location. 2. Upload the horizon.i386.pkg to directory \wnos\pkg\ on the file server.
- 3. Ensure that the value of the INI parameter autoload is not set to 0.
- 4. Restart the thin client and wait until the automatic installation of packages is complete. The installed horizon package is displayed in the **Packages** window in **System Tools**.

### Setting up the Skype for Business in VMware Blast session

This section describes how to install and use the Microsoft Skype for Business (SFB) on a VMware Blast desktop.

- 1. Log in as horizon administrator, and start the VMware Horizon Agent installation on the virtual desktop.
- 2. During the VMware Horizon Agent installation, select the VMware Horizon Virtualization Pack for Skype for Business option to install the VMware Horizon Virtualization Pack for SFB.

For Horizon Agent installation information, see the Setting Up Virtual Desktops in Horizon 7 document at docs.vmware.com.

The VMware Horizon Virtualization Pack for Skype for Business contains the following components:

- Horizon Media Proxy—This component is installed on the virtual desktop.
- Horizon Media Provider—This component is installed on the thin client.
- 3. Install the Skype for Business application on the VMware Blast desktop.
- Update the ThinOS firmware, and install the Horizon.i386.pkg on the ThinOS client. For more information about installing the Horizon package, see Installing Horizon package on ThinOS.
- 5. On ThinOS, log in to the VMware Blast desktop, and sign in to Skype for Business.

To verify if the VMware Horizon Virtualization Pack for Skype for Business is installed on the deployed virtual machines, check if the following registry keys exist:

- HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider GUID (REG SZ)
- HKEY LOCAL MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider GUID (REG SZ)

For information about pairing modes for a session, see the Configuring Skype for Business document at docs.vmware.com.

For information about configuring Skype for Business group policy settings, see the VMware Virtualization Pack for Skype for Business Policy Settings document at docs.vmware.com.

For information about the performance data statistics, see the Dell Wyse ThinOS Version 8.6 Release Notes at www.dell.com/support.

NOTE: To check the Skype for Business call statistics, right-click the virtualization pack icon on the lower-right of the virtual desktop, and click Call statistics.

#### Limitations

Horizon Client 4.8 or later and Horizon Agent 7.5 and later are not compatible with older Client and Agent releases. Due to this limitation, when you use the Horizon Client 4.8 and Horizon Agent 7.5 with older client and agent releases, Skype for Business calls run in fallback mode and calls are not optimized. For information about compatibility of Horizon Virtualization Pack for SFB components, see the article 54773 at kb.vmware.com.

• ThinOS uses the VMware binary. For information about the Skype for Business limitations, see the *Configuring Skype for Business* document at docs.vmware.com.

#### **Known issues**

#### Table 21. Known issues

Description	Workaround
If the Blast session resolution is higher than 1920 x 1080 during SFB calls with full screen, the mouse stops responding.	Do not use full screen during SFB calls in the blast session with resolution greater than or equal to 2560 x 1440.
On Wyse 5010, 5040, and 7010 thin clients, the performance is low during the Horizon SFB video call.	Do not use Horizon SFB video call on Wyse 5010, 5040, and 7010 thin clients.
After you install the JVDI package, the Trap 14 error occurs if you switch the playback device from HD audio to DP audio during the Horizon SFB call.	Do not load the JVDI package if you want to use only the Horizon package.
You cannot use the key on the headset to pick up or end a call.	There is no workaround in this release.

# Optimized mode and Fallback mode

In **Optimized mode**, the Skype for Business delivers an optimal performance. In **Fallback mode**, the Skype For Business calls are not optimized. On the lower right of the virtual desktop, the tooltip of the Virtualization Pack icon indicates the VMware Horizon Virtualization Pack for Skype for Business mode.

The following screenshot displays the Virtualization pack for Skype for Business in Optimized mode:



Figure 20. Optimized mode

If the Optimized mode icon is not displayed, the Virtualization Pack is running in Fallback mode. This is because of the version mismatch between the Horizon Client on the thin client and the Horizon Agent on virtual desktop.

For information about compatibility of Horizon Virtualization Pack for SFB components, see the *Horizon Client 4.8 or later and Agent 7.5* or later Virtualization Pack for Skype for Business is not compatible with older Client and Agent releases article at kb.vmware.com.

### Change Optimized mode to Fallback mode

To change the Optimized mode to Fallback mode, or to disable the Virtualization pack for Skype for Business on the Horizon desktop, do the following:

- 1. On the VMware Horizon desktop, open the Windows Registry Editor.
- 2. Rename the registry keys based on the following deployment scenarios:

Table 22. Registry keys

Deployment scenario	Registry key					
View Desktops (64-bit) with Skype for Business (64-bit)	Rename HKLM/Software/Microsoft/Office/Lync/ VdiMediaProvider to HKLM/Software/Microsoft/ Office/Lync/VdiMediaProviderDisabled.					
View Desktops (64-bit) with Skype for Business (32-bit)	Rename HKLM/Software/Wow6432Node/Microsoft/ Office/Lync/VdiMediaProvider to HKLM/Software/					

Table 22. Registry keys (continued)

Deployment scenario	Registry key					
	Wow6432Node/Microsoft/Office/Lync/ VdiMediaProviderDisabled.					
View Desktops (32-bit) with Skype for Business (32-bit)	Rename HKLM/Software/Microsoft/Office/Lync/VdiMediaProvider to HKLM/Software/Microsoft/Office/Lync/VdiMediaProviderDisabled.					

- 3. Close the Windows Registry Editor.
- Restart Skype for Business.
   Skype for Business is set to Fallback mode, and Real-Time Audio-Video (RTAV) is used for SFB calls.

# **Using multi-monitors in PCoIP session**

This section is applicable to Wyse 5070 thin client. ThinOS supports multiple-monitor display to run virtual machines on each monitor.

#### User scenario:

- 1. Connect multiple monitors to the ThinOS device.
- 2. In the Display Setup dialog box, disable Mirror Mode, and configure the display layout.
- 3. Launch a full screen PCoIP session.
- **Display numbers**—A virtual machine needs sufficient video memory to support three or four monitors. The default video memory on VMware vSphere supports only two monitors.
  - Supports one session up to four monitors in span mode with resolution up to 2560 x 1600.
  - o Supports one session up to two monitors in span mode with resolution up to 3840 x 2160.

The maximum number of monitors that can be stacked vertically is two. If you use more than two monitors, the monitors must be in the same mode and have the same screen resolution. For instance, if you use three monitors, all three monitors must be either in portrait mode or landscape mode, and must use the same screen resolution.

- **Display layout**—The display layout of the monitors must be aligned up and down, or left and right. Improper alignment results in unusual display.
- **3D rendering**—You can configure 3D graphics rendering for connected desktops. To use the 3D rendering feature, use up to two monitors with resolution up to 1920 x 1200.

Table 23. Matrix for multi screen support

					·	PCAIR	Multi-r	nonitor	suppor	+						
Wyse 50	70 Extended	l thin	client		<u> </u>	Con	- IVIGICI-I		suppoi							
	Resolution		192	20 x 12	00			256	0 x 144	10			3840 x 2160			
Display	No. of displays	Tw o	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
layout	Horizontal	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA	Yes	NA	NA	NA	NA
	Vertical	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA	Yes	NA	NA	NA	NA
	Grid	NA	Yes	Yes	NA	NA	NA	Yes	Yes	NA	NA	NA	NA	NA	NA	NA
Wyse 50	70 thin clien	t—Pe	entium				1									
	Resolution		192	20 x 12	00			256	0 x 144	10			384	0 x 216	0	
Display	No. of displays	Tw o	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
layout	Horizontal	Yes	Yes	NA	NA	NA	Yes	Yes	NA	NA	NA	Yes	NA	NA	NA	NA
	Vertical	Yes	Yes	NA	NA	NA	Yes	Yes	NA	NA	NA	Yes	NA	NA	NA	NA
Wyse 50	70 thin clien	t—Ce	eleron	-			-									

Table 23. Matrix for multi screen support (continued)

	PCoIP Multi-monitor support															
Display layout	Resolution	1920 x 1200			2560 x 1440				3840 x 2160							
	No. of displays	Tw o	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
	Horizontal	Yes	NA	NA	NA	NA	Yes	NA	NA	NA	NA	Yes	NA	NA	NA	NA
	Vertical	Yes	NA	NA	NA	NA	Yes	Na	NA	NA	NA	Yes	NA	NA	NA	NA

# **Using Multi-monitors in VMware Blast session**

This section is applicable to Wyse 5070 thin client. ThinOS supports multiple-monitor display to run virtual machines on each monitor.

**Prerequisite**: Update the VMware Blast package to the latest version. For more information, see the latest *Dell Wyse ThinOS Release Notes*.

#### User scenario:

- 1. Connect multiple monitors to the ThinOS device.
- 2. In the **Display Setup** dialog box, disable **Mirror Mode**, and configure the display layout.
- 3. Launch a full screen VMware Horizon Blast session.
- **Display numbers**—A virtual machine needs sufficient video memory to support multiple monitors. You can use up to four monitors with sufficient RAM.

Table 24. Display Layout matrix

Resolution	1920 × 1080					2560 × 1440				
No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
Horizontal	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA
Vertical	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA
Grid	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA

<sup>•</sup> **4K display**—ThinOS supports four displays with 4K resolution in a Horizon blast session. Due to low performance, Dell recommends that you do not use four displays with 4K resolution.

#### Table 25. 4K display support

Hardware version	Windows version	Number of 4K displays supported			
10 (ESXi 5.5.x compatible)	7, 8, 8.x, and 10	1			
11 (ESXi 6.0 compatible)	7—3D rendering feature and Windows Aero are disabled.	3			
11	7—3D rendering feature is enabled.	1			
11	8, 8.x, and 10	1			

- **3D rendering**—You can configure 3D graphics rendering for connected desktops. To use the 3D rendering feature, use up to two monitors with a resolution of up to 1920 x 1200. For a resolution of 4K (3840 x 2160), only one monitor is supported.
- Blast H.264—The following table describes the performance of H.264 decoder in VMware Horizon sessions that use the VMware Blast display protocol:

#### Table 26. Blast H.264 decoding

Screen resolution within VMware Horizon Blast session	Blast H.264 decoding in VMware Horizon Blast session	Summary		
Session display width is less than or equal to 1920 pixels.	Blast H.264 decoding is always enabled.	Horizon client uses Blast H.264 decoding even if the H.264 decoder setting is disabled using GUI or INI options.		

Table 26. Blast H.264 decoding (continued)

Screen resolution within VMware Horizon Blast session	Blast H.264 decoding in VMware Horizon Blast session	Summary
Session display width is greater than 1920 pixels.	Blast H.264 decoding is disabled by default. You can enable Blast H.264 decoding either on the ThinOS GUI or by deploying the INI parameter.	By default, Horizon client does not use Blast H.264 decoding. If the Blast H.264 decoder setting is enabled on ThinOS, then the Horizon client uses H.264 decoding. Enabling H.264 may downgrade the session performance.

For more information about the monitors and screen resolution, see the Monitors and Screen resolution section in the *Horizon 7 Architecture Planning* article at docs.vmware.com. However, Dell does not recommend that you use four displays with 4K resolution due to low performance.

# **Blast Virtual Printing**

Virtual printing with VMware Blast allows you to use local or network printers from the Blast desktop without the need of installing the additional print drivers on the remote desktop. For each printer configured locally on ThinOS, you must map the printer to the VMware Blast desktop. ThinOS Blast printer mapping is equivalent to VMware Blast virtual printing.

To map your printer, do the following:

- NOTE: LPT printer is considered as an example to explain the printer mapping scenario. Printer mapping in ThinOS works similar to LPT for LPD and SMB printers.
- Power on the ThinOS client with the VMware View broker configured in the Broker Setup tab. Set the connection protocol as All Supported from the Connection Protocol drop-down list.
- 2. Go to Global Connection Settings > Session, and retain the Exclude printer devices check box selection. This option is selected by default.
- 3. Plug in a USB printer to the ThinOS client terminal.
- **4.** Go to **System Setup** > **Printer**. The **Printer Setup** dialog box is displayed.
- 5. In the **Printer Setup** dialog box, do the following:
  - a. From the **Select Port** drop-down list, select **LPT 1**.
  - **b.** Enter valid printer name and printer identification.
  - c. Select the Enable the printer device check box.

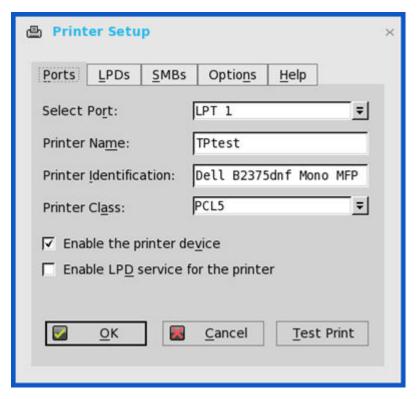


Figure 21. Printer Setup

- d. Click **Ok** to save the configuration.
- **6.** Click the **Options** tab, and do the following:
  - a. Set LPT1: <Printername>as default printer.
    - i NOTE: Do not select the Enable .print Client check box.
  - $\textbf{b.} \quad \text{Click } \textbf{Ok} \text{ to save the configuration.}$

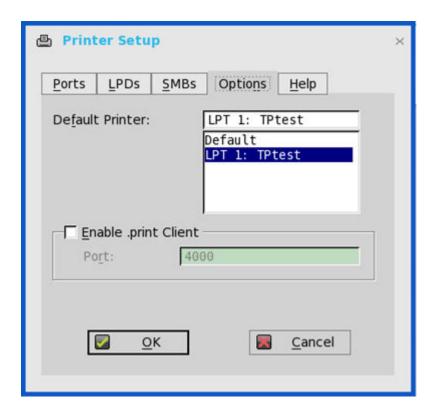


Figure 22. Options

7. Connect to a VMware Blast session. Go to **Control Panel** > **Devices and Printers**. The printer that is configured locally in ThinOS is mapped to the session.

The mapped printer's driver is TP PS Driver and the port is TPVM port.

The virtual printer allows the ThinOS local printer to be mapped to the VMware Blast session without installing the printer driver in the session.

### **Enable hardware cursor in Blast session**

The hardware cursor enables GPU to control the display of your mouse cursor. Hardware cursors have less latency.

ThinOS supports the hardware cursor in VMware Horizon session with Blast display protocol. Only two cursor colors—Black and White—are supported.

By default, the software cursor is used in a Blast session, and the hardware cursor is disabled. If the hardware cursor is not enabled, the cursor uses the true color. If the hardware cursor is enabled, the cursor uses black and white colors.

To enable the hardware cursor in a Blast session, use the following INI parameter:

 ${\tt SessionConfig=Blast\ EnableHardwareCursor=yes}$ 

### **Enable relative mouse feature**

The relative mouse feature is applicable for both PCoIP and Blast enabled thin clients. When you enable the relative mouse feature, Horizon Client uses relative coordinates to transmit data about the mouse pointer movement and improve the mouse performance. The relative mouse feature is supported on the following platforms:

- · Wyse 3030 LT thin client
- Wyse 3040 thin client
- · Wyse 5010 thin client
- · Wyse 5040 AIO thin client
- Wyse 5060 thin client
- Wyse 5070 thin client

#### For PCoIP enabled thin clients

To enable the relative mouse feature in the Classic mode, do the following:

- 1. Connect to a remote desktop using the PCoIP display protocol.
- 2. Right-click the remote desktop icon on the ThinOS taskbar.
- 3. Click Enable Relative Mouse.
  - NOTE: To disable the relative mouse feature, right-click the remote desktop icon on the ThinOS taskbar, and click Disable Relative Mouse.

To enable the relative mouse feature in the **Zero** mode, do the following:

- 1. Connect to a remote desktop using the PCoIP display protocol.
- 2. In the ThinOS connection menu, click the A icon that is displayed after the PCoIP session name.
- i NOTE: To disable the relative mouse feature, click the R icon that is displayed after the PCoIP session name.

#### For Blast enabled thin clients

- 1. Add SessionConfig=Blast EnableRelativeMouse=yes into the INI file.
- 2. Reboot the thin client.

You can see the entry [Horizon] enable relative mouse in the event log if Relative Mouse is enabled.

# **USB** device splitting in Blast session

ThinOS supports the USB device splitting feature on the Nuance Dictaphone PowerMic II microphone in a Blast session. The USB device splitting feature enables you to split the composite device into its components. To enable this feature, use the following INI parameters:

```
Device=vusb InterfaceRedirect=yes
Device=vusb ForceRedirect=0x00,0x00,0x00,0x00
SessionConfig=Blast viewusb.IncludeVidPid=Vid-0554_Pid-1001
viewusb.SplitVidPid=Vid-0554_Pid-1001(exintf:00;exintf:01;exintf:02)
```

After you enable the USB device splitting feature, the buttons on the PowerMic II are redirected to the blast session, and the audio mapping is retained in the local device.

For more information about the supported USB devices and USB configurations, see the *Nuance SpeechMagic VMware View Extension - Supported USB Devices and USB Configuration* article at kb.vmware.com.

# Supporting Teradici SDK

The PCoIP Client Software Development Kit (SDK) is a set of libraries and binaries that you can use to build or customize a PCoIP client.

ThinOS supports the Teradici SDK version 2.9.

#### User scenario:

- Behavior with earlier Teradici SDK versions: You were able to switch the USB disk redirection between sessions. For example, plug in the USB disk, and connect the desktop 1 and 2. The disk is redirected to desktop 1. If you disconnect from desktop 1, then the USB disk is redirected to desktop 2.
- Behavior with Teradici SDK version 2.9: When you disconnect from desktop 1, the USB disk is not redirected to desktop 2. You must remove the USB disk and plug in the USB disk again for redirection.

# Configuring PCoIP connections using Teradici Remote Workstation card

In ThinOS 8.6, you can directly configure the PCoIP connection using either the TERA2240 Remote Workstation Card or TERA2220 Remote Workstation Card. This feature is supported only on PCoIP-enabled thin clients. This feature only works with the direct PCoIP connection, and does not work when you connect using the Horizon View broker.

#### Prerequisites

· Ensure that the Teradici Remote Workstation card version matches the Teradici PCoIP SDK version 2.9.

- Ensure that host cards are connected to a remote workstation.
- · Ensure that host cards are installed correctly, that is, connected to a remote workstation with GPU.
- NOTE: The SDK in ThinOS does not function similar to Teradici zero client firmware. For example, the SDK in ThinOS does not support USB redirection with the host card connection. This feature is mainly for workstation users working on the server remotely.

To configure the PCoIP connection, do the following:

- 1. On ThinOS desktop, go to Connect Manager.
- 2. Click New, and then click PCoIP.

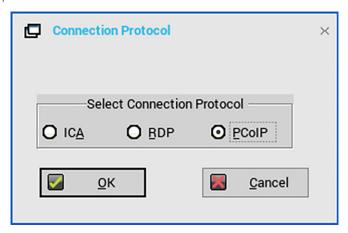


Figure 23. PCoIP Connection Protocol

3. In the Connection Settings (PCoIP) dialog box, do the following:

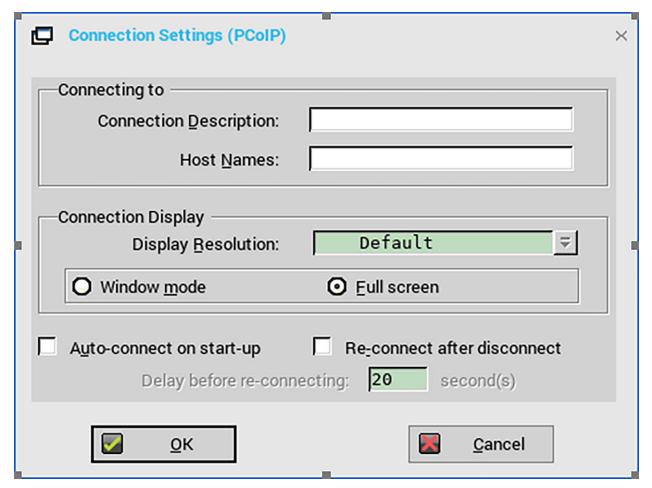


Figure 24. Connection Settings - PCoIP

- **a.** Enter the description for the PCoIP connection.
- **b.** Enter the IP address of the remote host card.
- c. From the Display Resolution drop-down list, select a display resolution for the PCoIP connection.
  TERA2220 supports a single display with 2560 x 1600 resolution or two displays with 1920 x 1200 resolution. TERA2240 supports two displays with 2560 x 1600 resolution or four displays with 1920 x 1200 resolution.
- d. Select either the Window mode or Full screen to set the initial view of the session.
- e. If you want to automatically connect to the session after you restart the thin client, select the **Auto-connect on start-up** check box.
- f. Select the **Re-connect after disconnect** check box if you want to automatically reconnect to a session after the session is disconnected. If you select this option, enter the wait interval in the **Delay before re-connecting** box. The default is 20 seconds.
- 4. Click **OK** to save the settings.

For more information about the supported platforms and limitations, see the *Dell Wyse ThinOS 8.6 Version Release Notes* at www.dell.com/support.

For information about the Teradici host cards, see the Host Card documentation at www.teradici.com.

# **Customize PCoIP login window and icons**

You can create customized PCoIP icons for the PCoIP login window on ThinOS using .png, .jpg, or .bmp files. This feature is available for the following platforms:

- · Wyse 3030 LT Thin Client with PCoIP
- Wyse 3040 Thin Client with PCoIP
- · Wyse 5010 Thin Client with PCoIP
- · Wyse 5040 AIO Thin Client with PCoIP
- Wyse 5060 Thin Client with PColP

- · Wyse 5070 Thin Client with PCoIP
- · Wyse 5470 Thin Client with PCoIP
- Wyse 5470 AIO Thin Client with PCoIP

To customize the broker agent window and icons, do the following:

1. To enable this feature, use the INI parameter SignOn=yes BitmapsMap={yes,no}

You must set BitmapsMap as yes for changing integrated bitmap images into customized bitmap images.

- 2. Place the text file **bitmaps.map** in the same folder as ThinOS builds.
  - NOTE: Similar to the PrinterMap file, each line in the file is of the format integrated bitmap file name = customized bitmap file.
- 3. Place the image files in the bitmap folder that is located inside the folder that contains ThinOS builds.

The following are some examples:

- m\_pcoip.ico=1-1\_16.png
- pcoip.ico=1-1\_32.png
- vdm.png=3\_355x85.png
- horizon\_wallpaper.jpg=Bugatti-Veyron-Wallpaper-Hd-1080p-uSa4W-1366x768.jpg

# **Configuring Microsoft Remote Desktop**

Microsoft Remote Desktop application allows you to access and manage the data and resources of a remote device using an internet connection. ThinOS supports RC4\_HMAC\_MD5 for RDP connections to compliment with AES128\_HMAC\_SHA1 or AES256\_HMAC\_SHA1.

This section provides information about how to configure the Remote desktop broker connection on your ThinOS device, and other remote desktop features that you can configure on ThinOS.

# Configuring the Microsoft Remote Desktop broker connection

To configure the Microsoft Remote Desktop broker setup:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

- 2. In the Broker Setup tab, from the drop-down list, select Microsoft, and do the following:
  - · Broker Server—Enter the IP address/Hostname/FQDN of the Broker Server.
  - Auto Connect List—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semi-colon, and is case-sensitive.
- 3. Click **OK** to save the settings.

# **Configuring RDP connections**

To configure the RDP connection:

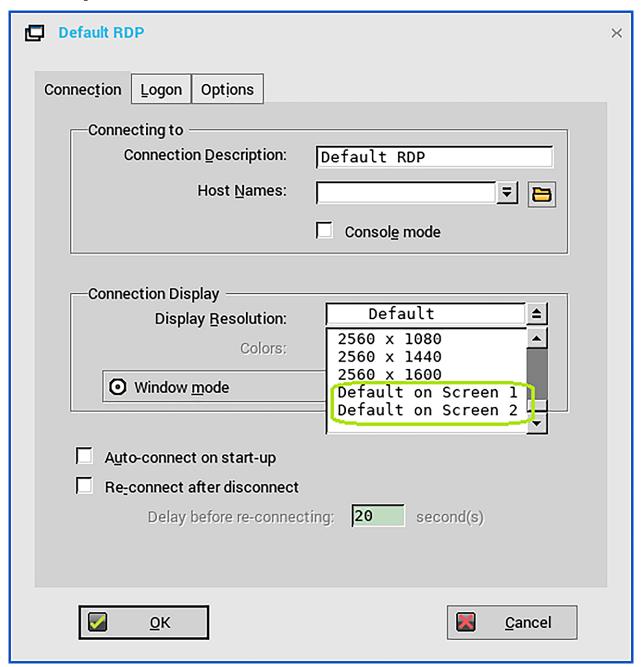
- From the desktop menu, click System Setup, and then click Remote Connections.
  The Remote Connections dialog box is displayed.
- 2. In the Broker Setup tab, from the drop-down list, select the Broker type as None.
- 3. Click  $\ensuremath{\textbf{RDP}}$  connection protocol, and click  $\ensuremath{\textbf{Configure}}.$

The **Default RDP** dialog box is displayed.

- 4. Click the Connection tab, and use the following guidelines:
  - a. Connection Description—Enter the descriptive name that is to appear in the connection list (38 characters maximum).
  - b. Host Names—Use the list to select the valid DNS server name or the IP address of the server to which the thin client connection is to be made. You can also use Browse next to the box to make the selection you want. For example, a list of WTS servers on the local network from which you can select.

- NOTE: The server name may be resolved using one of two mechanisms: DNS, and WINS. DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.
- c. Console mode—Select to set the RDP connection with Windows Console mode.
- d. **Display Resolution**—Select the display resolution for your RDP connection.

In ThinOS version 8.6, you can select your preferred monitor on which you want to start the RDP session in full screen mode based on the following scenarios:

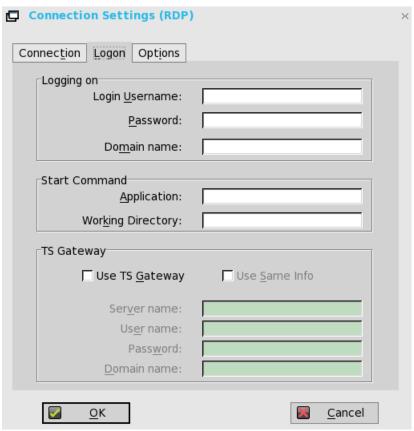


- Mirror mode is enabled on multi-display or single display—The Default on screen x option is not displayed. The display resolution of the RDP connection is set as **Default** irrespective of the value configured in the onscreen=x INI parameter.
- Span mode is enabled on multi-display—The Default on screen x option is displayed. You can select your preferred display on which you want to start the RDP session. You can also set your preferred display using the onscreen INI parameter. After you deploy the INI parameter, the Default on screen x option is set automatically according to the configured INI settings.

- NOTE: If the value defined in the onscreen parameter for your RDP connection is higher than the number of displays connected to the thin client, the display resolution is set as Default. If you switch the display mode between span and mirror, you must reboot the thin client to apply the INI settings.
- e. Colors—Select the color depth of the RDP session. If High Colors (16-bits) or True Colors (32-bits) is selected and the RDP server does not support this color depth, the thin client renegotiates the color depth to the lower value for example, 256 Colors (8-bits). The highest is 32-bits, if the hardware supports this color depth.
- f. Window mode on 1 monitor or Full screen span all monitors—Select the initial view of the session in window mode or full screen mode.
- g. Auto-connect on start-up—When selected, automatically connects the session on start-up.
- h. Re-connect after disconnect—When selected, causes the thin client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the **Delay before re-connecting** box (enter the number of seconds 1 to 3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds, if there is no INI file description of this connection, or is a Stand-alone user, or is simply omitted.

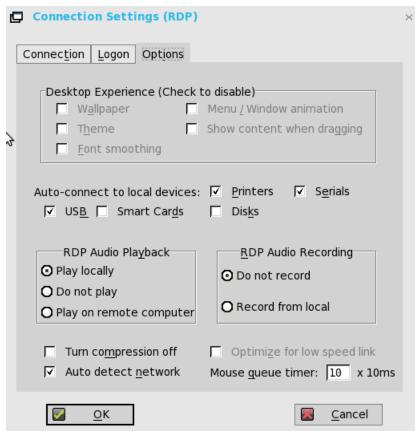
You can reset the options in the Connection tab of the Connection Settings (RDP) dialog box. To reset, click the **Reset VM** command button. This command button is located in the upper-right of the dialog box. It appears only with a VDM broker connection.

5. Click the **Logon** tab, and use the following guidelines:



- a. Logging on area—Enter login username, password, and domain name. If these boxes are not populated, you can enter the information manually in the RDP server login screen when the connection is made. Use the following guidelines:
  - Login Username Maximum of 31 characters is allowed.
  - · Password—Maximum of 19 characters is allowed.
  - **Domain Name**—Maximum of 31 characters is allowed.
- b. **Application** (127 characters maximum) and **Working Directory** (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.
- c. Use TS Gateway—Enables the use of Terminal Services Gateway (TS Gateway) server when connecting. If required, then enter the IP address or URL of the TS Gateway server in the Server name box. You can also enable Use Same Info (if the server credentials are the same credentials as your Remote Desktop Credentials (Host remote computer credentials) in the Login Username, Password, and Domain name fields) or disable Use Same Info and enter the Server name, User name, Password, and Domain name of the TS Gateway server if required.

- NOTE: A TS Gateway server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer with an Internet connection. A TS Gateway server enables Remote Desktop connections to a corporate network from the Internet without having to set up virtual private network (VPN) connections. Ask your network administrator whether you need to specify a TS Gateway server.
- · User Name—Enter a user name for the connection.
- Password—Enter the password.
- · **Domain**—Enter the domain name.
- NOTE: The user name, password, and domain name fields are optional. If you leave any of these fields blank, interactive login is required and users must enter the information at the login time.
- 6. Click **Options** tab, and use the following guidelines:



- a. Wallpaper—When selected, disables the desktop wallpaper.
- b. Menu / Window animation—When selected, disables the menu or window animation.
- c. Theme—When selected, disables the desktop themes.
- d. Show content when dragging—By default, when you grab a Window by the title bar and move it around, the contents of the window will move with it. Select this to disable this content view so that only the outline of the window moves when dragging it, until you drop the window. This option can be beneficial, as it uses less processing power.
- e. Font smoothing—Converts vector text to bitmap for better display.
- f. **Auto-connect to local devices**—Select any options (Printers, Serials, USB, Smart Cards, and Disks) to have the thin client automatically connect to the devices.
  - NOTE: USB—Redirects locally attached USB devices on the thin client to a Microsoft Windows terminal server. When the user connects to the terminal server, locally attached USB devices on the thin client are accessible.
- g. RDP Audio Playback—Select the audio playback options such as Play Locally, Do not play, and Play on remote computer.
- h. RDP Audio Recording—Select the audio recording options such as Do not record, and Record from local.
- $\textbf{i.} \quad \textbf{Turn compression off} \\ \textbf{-} \\ \textbf{When selected, turns compression off (intended for high-speed connections)}.$
- j. Optimize for low speed link—When selected, allows optimization for low-speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.
- k. Auto detect network—When selected, turns on the auto detect network feature. This feature is enabled by default. It also disables the Optimize for low speed link option and the Desktop Experience options by default.

- I. Mouse queue timer—Specifies the default queue timer of a mouse event in an ICA or RDP session (in 1/100 of a second). It can be used to adjust the bandwidth of a network.
- 7. Click **OK** to save the settings.

#### Switch between RDP session and ThinOS client desktop

After you start RDP sessions with the **Default on screen x** option, and you want to switch back to the ThinOS client desktop using Ctrl + Alt + Down key combinations, the design is as follows:

- Scenario 1: When the mouse cursor is located in an RDP session—In this scenario, if you press Ctrl + Alt + Down and select the
  user to log in to ThinOS, only the session with the mouse cursor is minimized and ThinOS desktop is displayed on the screen. Other
  RDP sessions remain unchanged.
- Scenario 2: When you start an RDP session on the primary display with Default on screen x—In this scenario, ensure that
  the RDP session on primary display has the mouse cursor. To switch back to the ThinOS desktop screen, press Ctrl + Alt +Down and
  select the user to log in to ThinOS.
- Scenario 3: When you press Ctrl + Alt + Down and select the System Information window—In the scenario, the window is displayed on the screen irrespective of the cursor position.
- Scenario 4: When you want to display the Connect Manager window—In this scenario, you must minimize the RDP session and open the ThinOS client desktop screen where the Connect Manager is located. Press Ctrl + Alt + Down and select Connect Manager.

#### Secure RDP

The default behavior does not allow connection to the server when the ThinOS RDP client fails to verify the server certificate. A security message is displayed indicating the failure. The following are the user INI parameters that can be used:

- · securitymode=high—a security message is displayed and the user is not allowed to connect to RDP.
- · securitymode=Warning—a security message is displayed but the user is allowed to connect to RDP.
- · securitymode=Low—the user is allowed to connect to RDP and no security message is displayed.

## Features of RDP protocol

Remote Desktop Protocol (RDP) is a network communications protocol developed by Microsoft that enables you to remotely access virtual desktops and applications. This section describes the functionality of ThinOS over RDP protocol.

## Using multi-monitors in RDP session

This section is applicable to Wyse 5070 thin client. ThinOS supports multiple-monitor display to launch RDP desktops on each monitor.

#### User scenario:

- 1. Connect multiple monitors to ThinOS device.
- 2. In the **Display Setup** dialog box, disable **Mirror Mode**, and configure the display layout.
- 3. Launch an RDP desktop with full screen.

All data described in the following table is based on virtual machine without RemoteFX/vGPU enabled configuration.

#### Table 27. RDP display capability matrix

Destination endpoint	Maximum resolution per monitor [Enable Force Span]	Maximum display support [Span Monitors]
Windows 7 SP1	4096 (w) x 2048 (h)	4096 (w) x 2048 (h)
Windows 8.1	8192 x 8192	6 x 4K
Windows Server 2012 R2	8192 x 8192	6 x 4K
Windows 10	8192 x 8192	6 x 4K
Windows Server 2016	8192 x 8192	6 x 4K

#### **RDP H.264**

From ThinOS version 8.5.1, logs of H.264 and H.264-AVC444 are hidden and not displayed in the **Event Log** tab. In ThinOS version 8.6, the H.264 resolution limitation is changed for different platforms.

The following table describes the RDP H.264 functionality matrix:

Table 28. RDP H.264 functionality matrix

RDP H.264	Session connection	Support platforms
H.264 is not enabled.	Windows 7/ Windows Server 2008 R2	All ThinOS-based platforms
H.264 is automatically disabled for display resolutions higher than 1920 x 1080.	Windows 8.x/ Windows Server 2012 R2, Windows 10/Windows Server 2016	Wyse 3010 thin client and Wyse 3020 thin client
H.264 is automatically disabled for display resolutions higher than 1920 x 1200.	Windows 8.x/ Windows Server 2012 R2, Windows 10/Windows Server 2016	Wyse 3040 thin client
H.264 is automatically disabled for display resolutions higher than 2048 x 1200.	Windows 8.x/ Windows Server 2012 R2, Windows 10/Windows Server 2016	Wyse 5060 thin client, Wyse 5470 thin client, and Wyse 5470 All-in-One thin client
H.264 is automatically disabled for display resolutions higher than 2048 x 1280.	Windows 8.x/ Windows Server 2012 R2	Wyse 3030 LT thin client, Wyse 5010 thin client, Wyse 5040 thin client, Wyse 7010 thin client, Wyse 5070 thin client
H.264 is automatically disabled for display resolutions higher than 3840 x 2160.	Windows 10/Windows Server 2016	Wyse 3030 LT thin client, Wyse 5010 thin client, Wyse 5040 thin client, Wyse 7010 thin client, Wyse 5070 thin client, Wyse 5470 thin client, and Wyse 5470 All-in-One thin client

The following table describes the RDP H.264 decoding matrix for Wyse 5070 thin client:

Table 29. RDP H.264 decoding matrix

Unit type	GPU	Session	Windows 10/W 20		Windows 8.1/W 2012	
		Display resolution	H.264- AVC444	Decoding	H.264	Decoding
		3840 x 2160	Enabled	Software	Disabled	
	AMD	2560 x 1440	Enabled	Software	Disabled	
	AIVID	2048 x 1280	Enabled	Software	Enabled	Hardware
M F070 F. I II III II II		1920 x 1200	Enabled	Software	Enabled	Hardware
Wyse 5070 Extended thin client	Intel	3840 x 2160	Enabled	Software	Disabled	
		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Hardware
		1920 x 1200	Enabled	Software	Enabled	Hardware
Wyse 5070 thin client—Celeron	Intel	3840 x 2160	Enabled	Software	Disabled	
processor Wyse 5070 thin client—Pentium		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Hardware
processor		1920 × 1200	Enabled	Software	Enabled	Hardware

All data described in the table is based on virtual machine without RemoteFX/vGPU enabled configuration.

### (i) NOTE:

- Windows 10/Window Server 2016 must be hosted in Microsoft RDS 2016 broker for enabling H.264-AVC444.
- H.264 logs and H.264-AVC444 logs are hidden and not displayed in the Event Log tab.

#### **Known issues**

In Mirror mode with active session, when you change the resolution from 2048 x 1280 to greater than 2048 x 1280, the connected RDP session (Windows 8/ Windows 2012 R2) is closed forcibly and an error message—RDP: The server-side graphics subsystem is in an error state and unable to continue graphics encoding is displayed. This is because the session is not reconnected in Mirror mode after resolution is changed that resulted in H.264 codec exceeding its supported resolution.

- Workaround—You must manually reconnect the session after the resolution is changed.
- In an RDP session with VOR enabled by default (Windows 8.1 x86), you connect to a session with full screen, and span more than four 4K monitors. In this scenario, if you play a video, the session may be disconnected automatically with an error log **RDP: The server-side graphics subsystem is in an error state and unable to continue graphics encoding**. This is because VOR /x-264 requires more resources, such as RAM, than the server resources.

Workaround—You can reduce the number of monitors or lower the resolutions or switch to other 64-bit operating system with more RAM.

### Configuring H.264 AVC444 in RDP 10 session

#### Prerequisites:

- · Thin client must run on ThinOS version 8.5 or later.
- · Windows 10 or Windows Server 2016 must be created in Microsoft RDS 2016 broker or in the latest VMware View broker.

### (i) NOTE:

H.264-AVC444 is also used in Windows 8.1 with RemoteFX GPU configured.

To configure the H.264 AVC444 in an RDP 10 session:

- 1. In the Windows session host, run gpedit.msc.
- 2. Open the Local Group Policy Editor.
- 3. Navigate to Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment, and enable the following policies:
  - Prioritize H.264/AVC 444 Graphics mode for Remote Desktop connections
  - · Configure H.264/AVC hardware encoding for Remote Desktop connections
- 4. Open cmd.exe and run gpupdate /force, or restart the server.

### VOR codec in RDP session

When you are playing video in an RDP session—Windows 8.1, Windows 2012 R2, Windows 10, and Windows 2016—VOR codec is used. The following logs are displayed in the **Event Log** tab.

```
System Information
                                    ENET
                  Event Log
                                           WLAN
General
        Copyright
                            Status
                                                   About
 01:31:26.689 RDP: Start session to 10.151.132.171
 01:31:26.689 RDP: Connect to 10.151.132.171
 G1:31:26.689 RDP: NLA CredSSP Authentication
 01:31:26.689 RDP: create network detection channel
 01:31:27.199 RDP: create UDP transportation
 01:31:49.954 TSMM: Media type audio/x-wma
 61:31:49.9/3 ISMM: Modia type video/x wmv
 61:31:50.495 VCR: Media Type video/x-264
 01:31:50.515 VOR: Media type video/x 264
```

Figure 25. Event log tab

### (i) NOTE:

- Dependence 1—RDP GFX status, H.264, and VOR work only when GFX is enabled.
- Dependence 2—VOR is dynamic. So the enablement/disablement of VOR dynamically changes during the change in the video resolution (enlarge/shrink).
- Dependence 3—H.264 enablement is decided at the beginning of connection, depending on the maximum resolution available for the session.

If H.264-AVC444 is enabled, VOR is not used in Microsoft broker 2016, and Windows 10/2016 sessions without the RemoteFX GPU. If you disable H.264-AVC444, VOR is used.

In RDP session (RDP 8.1 and later), VOR, H.264, and H.264-AVC444 are enabled by default. To disable these parameters, use the INI parameter— SessionConfig-RDP EnalbeGFX=yes EnableVOR=no EnableRDPh264=no.

When you connect to an RDP session in Windows 8.1 or Windows 10 with RemoteFX GPU adapter, H.264-AVC444 is used irrespective of the H.264-AVC444 group policy configurations. If you disable the H.264 feature by using the INI parameter, the VOR codec is used in RDP sessions. However, graphic-related issues are observed in RDP sessions. From ThinOS version 8.6, the VOR codec is not used when you disable H.264 using the INI parameter.

### **TS Gateway in Microsoft Broker**

#### User scenario:

- 1. Log in to Microsoft Broker with TS Gateway configured.
- 2. Launch a published collection.

TS Gateway connection is established.

The following table lists the TS Gateway versions supported by Windows Server.

#### Table 30. Supported TS Gateway versions

Server operating system	TS Gateway II	TS Gateway III	WebSocket
Windows 2008 R2	Support	Not support	Not Support
Windows 2012 R2	Support	Support	Not Support
Windows 2016	Support	Support	Support

### (i) NOTE:

- TS Gateway WebSocket is a new feature introduced from ThinOS version 8.5.
- In TS Gateway II or III connection, the setup uses a two half-duplex communication between Terminal Server (TS)
  Gateway server and thin client.
- In the WebSocket connection, the session connection setup uses a duplex communication between TS Gateway and thin client
- TS Gateway II and TS Gateway III are downward compatible with Windows Server 2016, that means, if the WebSocket connection fails or the TS Gateway server or thin client version does not support WebSocket, then TS Gateway II or TS Gateway III is used.

The following screenshot displays the TS Gateway II connection setup logs:

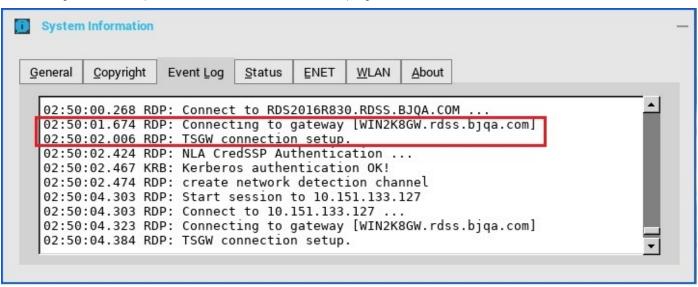


Figure 26. Event log tab

The following screenshot displays the TS Gateway III connection setup logs:

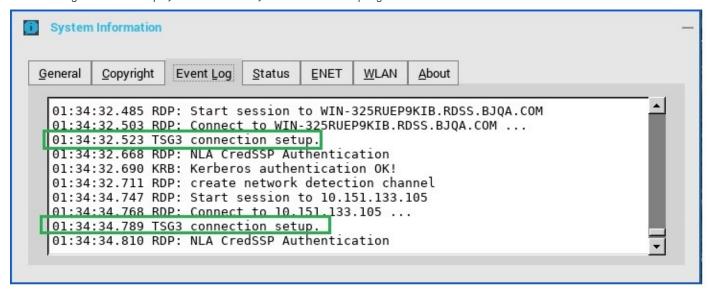


Figure 27. Event log tab

### (i) NOTE:

- WebSocket connection log is hidden and not displayed in the Event Log tab. If you want to view the WebSocket connection log, go to Troubleshooting > Capture and enable Persistent for the export event log.
- From the ThinOS v8.6 release onwards, the WebSocket feature is disabled by default. To enable WebSocket, deploy
  the following INI parameter:

Sessionconfig=RDP TSGWWebSock=yes.

### Connect to RDP session using UDP with TS Gateway

To connect to a Remote Desktop Session using User Datagram Protocol (UDP) with TS Gateway, do the following:

- Deploy the following INI parameter to the thin client: SessionConfig=RDP TSGWUDP=yes.
- 2. Enable **Terminal Services Gateway** (TSGW) for the applications and desktops from the Microsoft RDS broker server.
- 3. On the ThinOS client, start a Remote Desktop Session using the RDS connection broker.
- 4. Connect to the published desktop.

On the ThinOS desktop, the following event log is displayed in the **System Information** window:

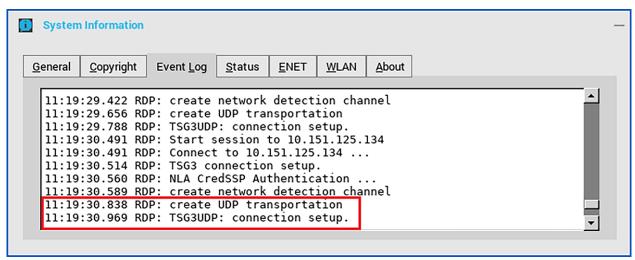


Figure 28. Event log

# Configuring Dell vWorkspace

Workspace virtualization delivers a list of applications or desktops together as a single complete virtual workspace. It isolates and centralizes an entire computing workspace, vWorkspace provides flexible, location and platform independent access by delivering virtual workspace from multiple virtualization platforms.

This section provides information about how to configure a Dell vWorkspace broker connection on your ThinOS device.

# Configuring the Dell vWorkspace broker connection

To configure the vWorkspace broker setup:

- 1. From the desktop menu, click System Setup, and then click Remote Connections.
  - The **Remote Connections** dialog box is displayed.
- 2. In the Broker Setup tab, from the drop-down list, select Dell vWorkspace, and do the following:
  - · Broker Server—Enter the IP address/ Hostname/ FQDN of the Broker Server.
  - Auto Connect List—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be listed. Each desktop name is separated by a semi-colon, and is case-sensitive.
  - · Select the check box to enable vWorkspace Gateway.
  - · **vWorkspace Gateway**—Enter the IP Address of the vWorkspace Gateway.
- 3. Click **OK** to save the settings.

# Configuring Amazon Web Services or WorkSpaces

Amazon WorkSpace is a cloud-based virtual desktop that allows you to access remote applications with ease.

Amazon WorkSpaces connection is applicable only for PCoIP clients running ThinOS 8.3, and later versions.

This section provides information about how to configure the Amazon WorkSpaces (AWS) connection on your ThinOS device, and other Amazon WorkSpace features that you can configure on ThinOS.

# Configuring the Amazon WorkSpaces broker connection

Amazon WorkSpaces connection is applicable only for PCoIP clients. To configure the Amazon WorkSpaces (AWS) broker setup:

- From the desktop menu, click System Setup, and then click Remote Connections
   The Remote Connections dialog box is displayed.
- 2. In the Broker Setup tab, from the Select Broker Type drop-down list, select Amazon WorksSpaces.

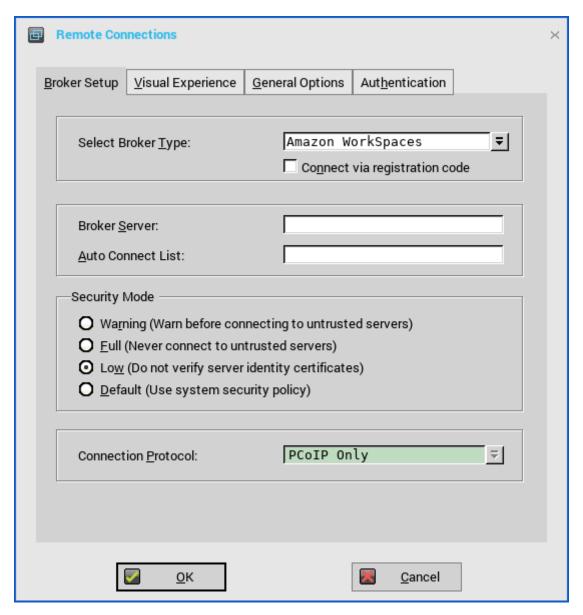


Figure 29. Amazon WorkSpaces

- 3. Based on your preferred connection mode, do either of the following:
  - If you want to connect to AWS using the registration code, select the Connect via registration code check box, and enter the WorkSpaces registration code in the Registration Code field. The workspace registration code is provided to you in your welcome email after you set up Amazon WorkSpaces.

You can also use the INI parameter UseRegistrationCode=yes to connect to AWS using a registration code. The check box is selected automatically if you enable the option using the INI parameter.

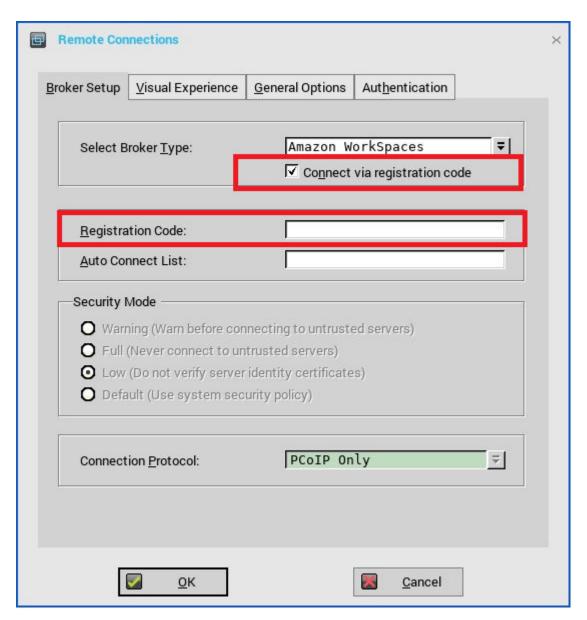


Figure 30. Amazon WorkSpaces with the Registration Code field

## NOTE: You cannot configure the direct connection mode using the INI parameter or Wyse Management Suite.

ThinOS enables you to modify the registration code anytime from the Amazon WorkSpaces (AWS) login window. This feature is applicable if you are connecting to AWS using the registration code. Deploy the INI parameter  $EnableAWSREGCode=\{yes, no\}$  to use this feature.

· If your server supports Multi-factor authentication (MFA), use the following INI parameter:

ConnectionBroker=AWS Host=wsnrt+KQRQWM UseRegistrationCode=yes EnableMFA=yes

The MFA token field is enabled. Use the Google Authenticator on your mobile device and enter the code that is generated.

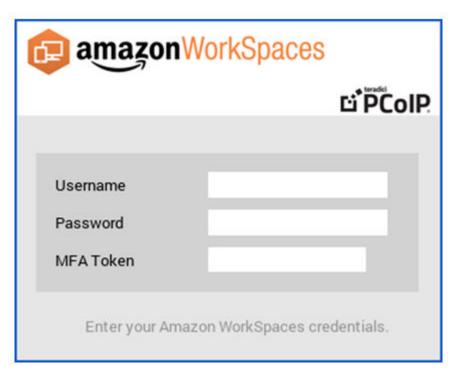


Figure 31. Amazon WorkSpaces login window for servers that support MFA

If your server does not support MFA, use the following INI parameter:

ConnectionBroker=AWS Host=wsnrt+KQRQWM UseRegistrationCode=yes EnableMFA=no



Figure 32. Amazon WorkSpaces login window for servers that do not support MFA

- If you want to connect to AWS using the default PCoIP Gateway mode, enter the IP address/Hostname/FQDN of the broker server in the **Broker Server** field.
  - NOTE: Do not select the Connect via registration code check box if you are using the default PCoIP Gateway mode.
- **4.** In the Auto Connect List field, enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be listed. Each desktop name is separated by a semicolon, and is case-sensitive.
- **5.** Select the preferred Security mode from the following options:
  - Warning—This security mode requires FQDN address for domain certificate that is installed in PCM. If certificate is not installed
    on the client, corresponding warning message is displayed for you to continue.

- Full—This security mode requires FQDN address with domain certificate that is installed in PCM, and certificate installed on the client.
- · Low—This security mode enables FQDN/IP address with/without certificate.
- Default—Follows global security mode settings.
- NOTE: The Connection Protocol drop-down list is disabled for the AWS broker. By default, the option is set to PCoIP Only.

#### 6. Click OK

For information about deploying AWS WorkSpaces and AWS EC2 PCM for AWS WorkSpaces, go to www.teradici.com/web-help/Connecting\_ZC\_AWS\_HTML5/TER1408002\_Connecting\_ZC\_AWS.htm#03\_DeployPCM.htm%3FTocPath%3D3.

For information about configuring the Broker Server address = "URI (https://<FQDN or IP address>) of the PCM", go to www.teradici.com/web-help/Connecting\_ZC\_AWS\_HTML5/TER1408002\_Connecting\_ZC\_AWS.htm#05\_Connect.htm %3FTocPath%3D5.

#### Known issues with Amazon Web Services or WorkSpaces

- Key combination Ctrl + Alt disconnects users from AWS session intermittently with old agent in AWS desktop. To fix this issue, update to latest agent by rebooting the desktop.
- Each user is assigned with one WorkSpaces desktop, and therefore logon with any username returns to the single desktop and then the session connects automatically. Disconnecting from the desktop returns user to logon screen.

# **Configuring Teradici Cloud Access**

Teradici technology enables you to securely access the remote applications using Teradici Cloud Access. You can manage and optimize your PCoIP-enabled clients. For more information about Cloud Access, see <a href="https://www.teradici.com/cloud-access">www.teradici.com/cloud-access</a>.

NOTE: You can use the INI parameter *ConnectionBroker=TeradiciCloudAccess* to enable Teradici cloud access from this release. The INI parameter sets Teradici as the connection broker.

This section provides information about how to configure a Teradici Cloud Access broker connection on your ThinOS device.

# Configuring the Teradici Cloud Access broker connection

To configure the Teradici Cloud Access broker setup:

From the desktop menu, click System Setup, and then click Remote Connections.
 The Remote Connections dialog box is displayed.

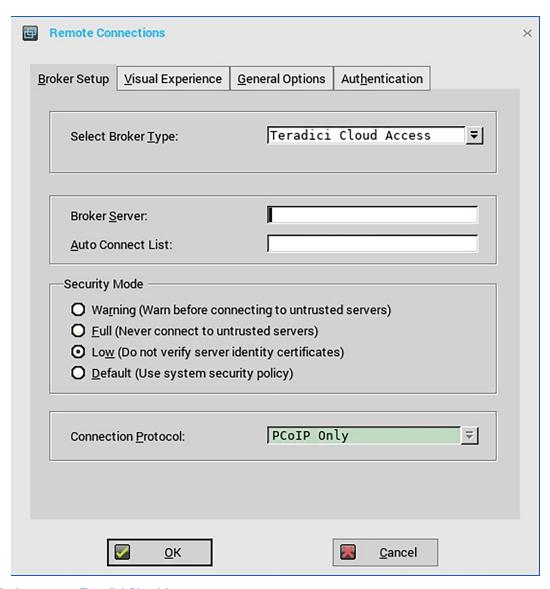


Figure 33. Broker setup - Teradici Cloud Access

- 2. On the **Broker Setup** tab, from the **Select Broker Type** drop-down list, select **Teradici Cloud Access**, and configure the following options:
  - **Broker Server**—Enter the IP address or FQDN of the broker server.
  - **Auto Connect List**—Enter the name of desktops that you want to start automatically after logging in to the respective broker. Use a semicolon to separate each desktop name.
    - i NOTE: Field values are case-sensitive.
  - **Security mode**—Select your preferred security mode from the following options:
    - **Warning**—Warn security requires the FQDN address with a self-signed certificate, or without any certificate. However, the corresponding warning message is displayed.
    - o **Full**—Full security requires the FQDN address with a domain certificate.
    - o **Low**—Low security allows the FQDN or IP address with or without a certificate.
    - o **Default**—Follows the global security mode settings.
  - Connection Protocol—By default, the option is set to PColP Only.
- 3. Click **OK** to save your settings.

# **Configuring local settings**

You can configure available thin client settings on the thin client using the following. Depending on user privilege level, some dialog boxes and options may not be available for use.

NOTE: While it is not recommended to use dialog boxes for configuring thin client settings, they are available in case you want to temporarily override central default configurations or you do not have the option to set up central configuration (smaller environments). In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all supported thin clients in your environment.

# **Local Settings Menu**

To access the Local settings menu:

- Zero desktop—Click the System Settings icon on the Zero toolbar. Administrators can also click the Admin Mode button on the Login dialog box.
- · Classic desktop—Click User Name, and select System Setup.
- i NOTE: User Name is the user who is logged-on and is at the lower-left pane of the taskbar.

## Configuring the system preferences

Use the **System Preference** dialog box to select personal preferences such as screen saver, time/date and custom information settings.

### Setting the general system preference

To configure the general settings for system preference:

- From the desktop menu, click System Setup, and then click System Preferences.
   The System Preference dialog box is displayed.
- 2. Click the **General** tab, and use the following guidelines:
  - a. Battery or Plugged in—This step is only applicable for Wyse 5470 and Wyse 5470 All-in-One thin clients. Select the Battery option if the device runs on battery. Select the Plugged in option if the device is connected to an external power source.
    - i NOTE: On the Wyse 5470 All-in-One Thin Client, only the Plugged in option is available.
  - **b. Screen Saver**—Allows you to select the type of screensaver you want. The default is to **Turn Off Screen**.
    - Other available screensavers are Flying Bubbles, Moving Image, Showing Pictures, and Playing Video.
  - Timer—Select the idle time after which the screensaver is to be activated; either disable, 1 minute, 3 minutes, 5 minutes, 10 minutes (default), 15 minutes, or 30 minutes.
    - When the thin client is left idle for the specified idle time, the screensaver is initiated.
  - d. After Turn Off Screen—Specify whether the thin client must enter the sleep mode or power off after the screen is turned off by the screen saver. This option is available only on Wyse 5040 AIO clients.
  - e. Timer—Select the idle time after which you need the thin client to enter sleep mode. This option is available only on Wyse 5040 AIO clients.
  - f. Locale—Select a language to be activated for the user login-experience; either French, German, Korean, or English.
    - NOTE: Locale changes the language for the user login-experience screens only displayed during boot-up and login and not the configuration or administrator screens.

Only the following messages are applicable for French locales:

- · Username/Password/Domain
- · System Information
- $\cdot$  Shut down the system, restart the system, reset the system setting to factory default
- · OK, Cancel

- · Initiating devices
- · Looking up IP address from DHCP, Note: Pressing CTRL-ESC keys cancel out of network check
- · Retry DHCP for an IP address
- · Waiting for network link. Verify that network cable is plugged into back of unit
- · Check Cable, No Ethernet link
- · Leave administrator mode
- Connecting
- · Sign off from account
- · Lock Terminal, Unlock Password
- · Terminal is locked, Invalid unlock password
- g. **Terminal Name**—Allows you to specify the name for the thin client. The default is a 14-character string that is composed of the letters WT followed by the thin client Ethernet MAC address.

Some DHCP servers use this value to identify the IP address lease in the DHCP Manager display.

3. Click **OK** to save the settings.

The Wyse 5470 Thin Client behaves in the following manner when the lid is closed:

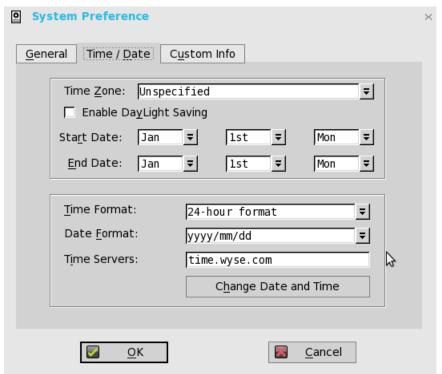
- · With the AC adapter plugged in—Closing the lid turns off all displays including the external displays.
- · Without the AC adapter plugged in—Closing the lid turns off the system.

You can change the close lid behavior by using the INI parameters. For more information about the INI parameters, see the Dell Wyse ThinOS INI Reference Guide at www.dell.com/support.

### Setting the time and date

To configure the time and date settings:

- From the desktop menu, click the System Setup, and then click System Preferences.
   The System Preference dialog box is displayed.
- 2. Click the **Time/Date** tab, and use the following guidelines:



- a. Time Zone Select a time zone where the thin client operates from the drop-down list. Default value is Unspecified.
- b. **Enable Daylight Saving** Allows you to enable the daylight saving settings. When selected, the **Start Date** and **End Date** boxes must be properly configured to define the daylight saving starting (month/week/day) and ending (month/week/day) periods.

Use the following guidelines to enter the Start date and End date:

Month— Specifies the month in the year from January through December.

- · Week Select 1 through 4 for the week in the month. Week last denotes the last week in the month.
- Day Specifies the day of the week from Monday through Sunday.
- c. Time Format Allows you to select the 12 or 24-hour time format. default is 24-hour format.
- d. Date Format Allows you to select the yyyy/mm/dd (year/month/day) or dd/mm/yyyy (day/month/year) date format.
   Default is yyyy/mm/dd.
- e. Time Servers List of IP addresses or host names with optional TCP port number of Time Servers.

Each entry with optional port number is specified as Name-or-IP: port, where: port is optional. If not specified, port 80 is used. Locations can be supplied through user profiles if user profiles are used. The Time Servers provide the thin client time based on the settings of time zone and daylight saving information. If DHCP is used, locations can be supplied through DHCP.

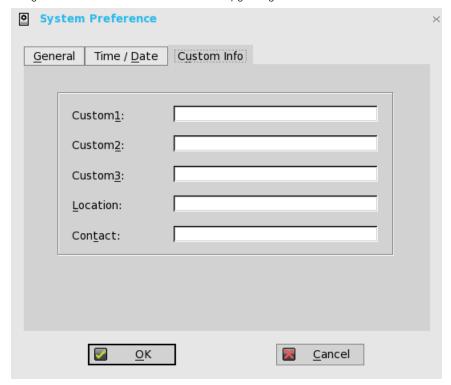
- f. Change Date and Time Allows you to change date and time for secure environments requiring a solution to outside server access. When connecting to a file server over HTTPS, the proper time must be defined on the thin client for SSL/ certification validation.
- 3. Click **OK** to save the settings.

### **Setting the custom information**

Use the **Custom Info** tab to enter configuration strings for use by WDM software. The configuration strings can contain information about the location, user, administrator, and so on.

To set the custom information:

- From the desktop menu, click System Setup, and then click System preferences.
   The System preference dialog box is displayed.
- 2. Click the **Custom Info** tab to enter configuration strings used by WDM software. The configuration strings can contain information about the location, user, administrator, and so on. Clicking **OK** transfers the custom field information you enter in the dialog box to the Windows registry. The information is then available to the WDM Client Manager. For more information on using Custom Fields and using WDM for remote administration and upgrading thin client software, see WDM documentation.



3. Click **OK** to save the settings.

# Configuring the display settings

Use the **Display** dialog box to select the resolution and refresh rate for the monitor used with the thin client.

## Configuring the display setup

This section is applicable to Wyse 5070, Wyse 5470, and Wyse 5470 All-in-One thin client. Use the **Display Setup** dialog box to configure the display settings for the connected monitors.

To configure the display setup:

- i NOTE: On Wyse 5470 Thin Client, the built-in display stays on by default.
- From the desktop menu, click System Setup, and then click Display.
   The Display Setup dialog box is displayed.
- 2. In the **Display Setup** dialog box, configure the following options:
  - Mirror mode
    —Select the Mirror mode check box to enable all connected monitors to use the same display settings configured
    on the primary monitor.

The following screen represents the Mirror mode configuration.

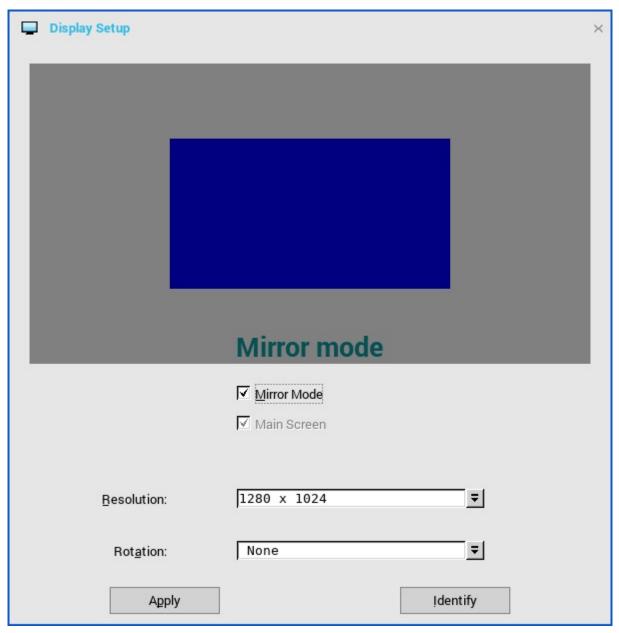


Figure 34. Display settings

If you clear the **Mirror mode** check box, the **Span Mode** is enabled. The following screen represents the span mode configuration.

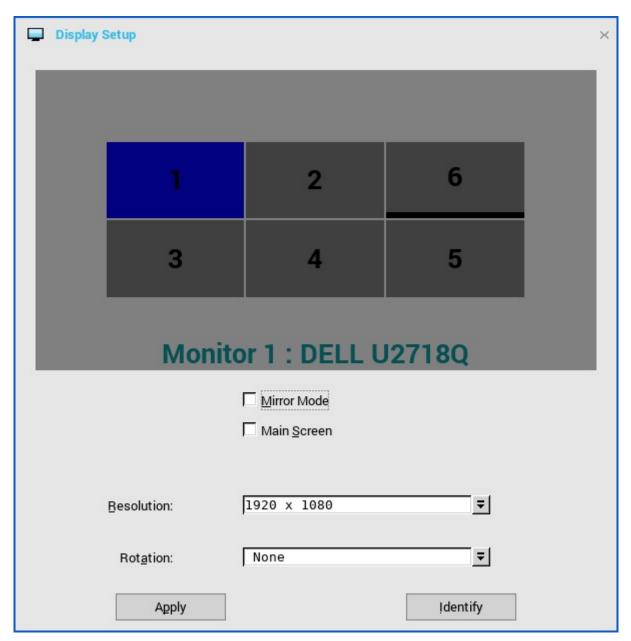


Figure 35. Display settings

Blocks displayed on the screen represent the number of monitor screens connected to the thin client. Each block represents a single monitor screen.

Every monitor contains a unique display order number and display configuration. You can move the blocks horizontally or vertically and construct the multi-display layout in mixed directions. To construct a new display layout, move the blocks to your preferred position, and click **Apply**. A new display layout is created. However, the system sets the block to its default position if the block is moved to an incorrect position.

### (i) NOTE:

- The Wyse 5070 Extended thin client supports up to six monitors.
- The Wyse 5470 Thin Client supports up to three simultaneous displays.
- Main screen—Select the Main screen check box to set the monitor as primary monitor or main screen. To set a monitor as main screen, click the monitor block, and select the Main screen check box. After you set the monitor as main screen, the monitor block is highlighted with an underline, and the Main screen option is disabled for that monitor block. The Main screen option is available for other monitor blocks.
  - i NOTE: Main screen option is effective only in Span Mode and always disabled in Mirror Mode.
- Resolution—From the Resolution drop-down list, select a display resolution supported by your monitor.

NOTE: The default screen resolution on the Wyse 5470 Thin Client is  $1366 \times 768$  or  $1920 \times 1080$  depending on the configuration. The default screen resolution on the Wyse 5470 All-in-One Thin Client is  $1920 \times 1080$ .

In Mirror Mode, the resolution list is derived from the intersection of resolutions in all connected monitors.

- In Span Mode, select a monitor block and change its resolution from the Resolution drop-down list.
- Rotation—From the Rotation drop-down list, select an option to rotate the monitor screen in different directions—Left turn 90 degrees or Right turn 90 degrees. By default, the option is set to None.
- 3. Click Apply.
  - The new display settings are applied, and you can view the modified display.
- 4. Click **OK** to confirm the new settings.
- i NOTE: Use the Identify option, to know the display order number of the connected monitors.

### Hardware capability

This section describes the hardware capability for display.

### Table 31. Port preferences

Model	Summary
Wyse 5070 thin client with Celeron processor	<ul> <li>On Wyse 5070 thin client without wireless module, the optional port can be used as second RJ-45, SFP, VGA, or second serial port.</li> <li>On Wyse 5070 thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP.</li> <li>When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive.</li> </ul>
Wyse 5070 thin client with Pentium processor	<ul> <li>On Wyse 5070 thin client without wireless module, the optional port can be used as second RJ-45, SFP, VGA, or second serial port.</li> <li>On Wyse 5070 thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP.</li> <li>Back headset is disabled if front headphone is used.</li> <li>When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive.</li> <li>When VGA monitor is connected on VGA optional port, DisplayPort 3 becomes inactive.</li> </ul>
Wyse 5070 Extended thin client	<ul> <li>On Wyse 5070 Extended thin client without wireless module, the optional port can be used as second RJ-45, SFP, or VGA.</li> <li>On Wyse 5070 Extended thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP.</li> <li>Back headset is disabled if front headphone is used.</li> <li>When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive.</li> <li>When VGA monitor is connected on VGA optional port, DisplayPort 3 becomes inactive.</li> <li>Power option is available on the first serial port.</li> <li>PCle slot is available.</li> </ul>

#### Wyse 5070 thin client with Celeron processor

### Table 32. Display matrix

Number of displays	Supported display resolution			
	4K resolution	Non-4K resolution		
	3840 x 2160 @ 60 Hz	Up to 2560 x 1600 @ 60 Hz		
One display	Yes	Yes		
Two displays	Yes	Yes		
Three displays	No <sup>1</sup>	Yes²		

<sup>&</sup>lt;sup>1</sup>VGA port does not support 4K display. However, it supports a display with 1080p screen resolution.

<sup>2</sup>For non-4K displays, screen resolution up to 2560 x 1600 @ 60 Hz is supported on all ports except VGA. VGA port supports only 1080p resolution.

#### Table 33. Ports

Ports	DP1	DP2	VGA	USB Type-C
Monitor priority	1	2B¹	3	2A1
4K display	Yes	Yes	No²	Yes
Non-4K display	Yes	Yes	Yes²	Yes

<sup>&</sup>lt;sup>1</sup>DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

NOTE: 4K resolution @ 60 Hz on USB-C type port is tested using the Type-C to HDMI and DP adapters. Dell monitor S2718D with USB type-C port supports up to 2560 x 1440 resolution.

#### Wyse 5070 thin client with Pentium processor

#### Table 34. Display matrix

Number of displays	Supported display resolution			
	4K resolution	Non-4K resolution		
	3840 x 2160 @ 60 Hz	Up to 2560 x 1600 @ 60 Hz		
One display	Yes	Yes		
Two displays	Yes	Yes		
Three displays¹	Yes	Yes		

<sup>&</sup>lt;sup>1</sup>Dell recommends that you configure a maximum of two displays with 4K resolution and the third display with non-4K resolution on DisplayPort 3 for optimized stability and performance. However, based on the maximum technical capability of Wyse 5070 thin client with Pentium processor, ThinOS supports a maximum of three 4K displays.

#### Table 35. Ports

Ports	DP1	DP2	DP3	VGA	USB Type-C
Monitor priority	1	2B1	3B <sup>2</sup>	3A²	2A¹
4K display	Yes	Yes	Yes	No³	Yes
Non-4K display	Yes	Yes	Yes	Yes³	Yes

<sup>&</sup>lt;sup>1</sup>DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

NOTE: 4K resolution @ 60 Hz on USB-C type port is tested using the Type-C to HDMI and DP adapters. Dell monitor S2718D with USB type-C port supports up to 2560 x 1440 resolution.

#### Wyse 5070 Extended thin client with AMD GPU

#### Table 36. Wyse 5070 Extended thin client with AMD GPU

Number of displays	Supported display resolution		
	4K resolution	Non-4K resolution	
	3840 x 2160 @ 60 Hz	Up to 2560 x 1600 @ 60 Hz	
One display	Yes	Yes	
Two displays	Yes	Yes	

<sup>&</sup>lt;sup>2</sup>VGA port supports only 1080p resolution.

<sup>&</sup>lt;sup>2</sup>DP3 and VGA port are mutually exclusive with VGA port taking higher priority.

<sup>&</sup>lt;sup>3</sup>VGA port supports only 1080p resolution.

Table 36. Wyse 5070 Extended thin client with AMD GPU (continued)

Number of displays	Supported display resolution		
Three displays <sup>1</sup>	Yes	Yes	
Four displays²	Yes	Yes	
Five displays²	Yes	Yes	
Six displays²	Yes <sup>2</sup>	Yes	

<sup>&</sup>lt;sup>1</sup>For three displays, Dell recommends that you configure the first two 4K displays on the main board (DP1~DP3), and the third 4K display on AMD GPU card.

NOTE: Best practice—To achieve maximum 4K display output, Dell recommends setting up 1080p on the DisplayPort 3, with rest of the monitors in 4K resolution to optimize performance.

Table 37. Ports

Ports	DP1	DP2	DP3	VGA	USB Type-C	mDP4	mDP5	DP6
Monitor priority	1	2B¹	3B²	3A²	2A¹	4	5	6
4K display	Yes	Yes	Yes	No³	Yes	Yes	Yes	Yes
Non-4K display	Yes	Yes	Yes	Yes³	Yes	Yes	Yes	Yes

<sup>&</sup>lt;sup>1</sup>DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

NOTE: 4K resolution @ 60 Hz on USB-C type port is tested using the Type-C to HDMI and DP adapters. Dell monitor S2718D with USB Type-C port supports up to 2560 x 1440 resolution.

<sup>&</sup>lt;sup>2</sup>Dell recommends that you configure a maximum of four displays with 4K resolution and the remaining displays with non-4K resolution on DisplayPort 3 and DisplayPort 6 for optimized stability and performance. However, based on the maximum technical capability of Wyse 5070 Extended thin client, ThinOS supports a maximum of six 4K displays.

<sup>&</sup>lt;sup>2</sup>DP3 and VGA port are mutually exclusive with VGA port taking higher priority.

<sup>&</sup>lt;sup>3</sup>VGA port supports only 1080p resolution.

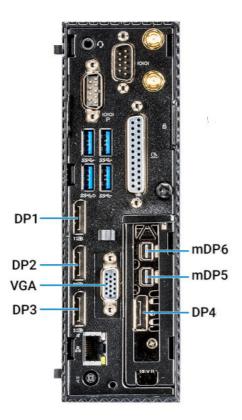


Figure 36. Ports on Wyse 5070 Extended thin client

**Monitor priority**—The following order defines the monitor priority set on ThinOS for Wyse 5070 Extended thin client:

- DP1 > DP2 > DP3 > DP4 > mDP5 > mDP6
- DP1 > USB Type-C > DP3 > DP4 > mDP5 > mDP6
- DP1 > DP2 > VGA > DP4 > mDP5 > mDP6
- DP1 > USB Type-C > VGA > DP4 > mDP5 > mDP6
- NOTE: Monitor cable hot plug—Screen layout settings are changed based on supported monitor resolution and the port to which the monitor is plugged in.
- NOTE: Earlier in ThinOS zero theme, the Display Setup window was aligned with left-hand setting panel. In current scenario, the Display Setup window is positioned to center of the screen regardless of Classic/Zero mode. This enhancement is made to easily configure the display setup along with the confirmation window.

### Known issues

- Hot plugging a monitor may result in a black screen in the VDI connected session. To recover the session screen, you must power off
  the monitor, and then power on the monitor. This issue will be resolved in the next release.
- Hot plugging a monitor during VDI connection or display setup configuration may result in unexpected issues, such as terminal freeze
  or display layout change. This issue will be resolved in the next release.

#### Port preferences on the Wyse 5470 Thin Client

- · HDMI, DisplayPort over USB Type-C, and USB Type-C ports are prioritized over the VGA port.
- · When a USB Type-C display is present, there is no display on the VGA port.
- · If a VGA display is present, a third display that is connected is prioritized and the VGA display is turned off.
- · If a VGA display is not present, a third display that is connected is ignored, or a blank screen is displayed on the third screen.

### Using the On-Screen Display (OSD)

This section is applicable to Wyse 5470 All-in-One thin client.

Use the On-Screen Display (OSD) buttons on the right of the device to adjust the luminance of the backlight. Minimum is 1 and maximum is 100.

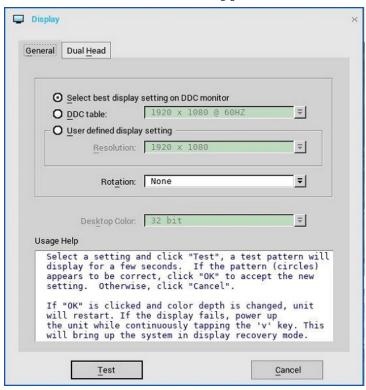
- Press and hold the first button from the top to increase brightness.
- · Press and hold the second button from the top to decrease brightness.
- Press the screen-off button to turn off or turn on the display. When the display is turned off, you can use a mouse or a keyboard to wake up the thin client.

### Configuring the general display settings

This section is not applicable to Wyse 5070 thin client.

To configure the general display settings:

- From the desktop menu, click System Setup, and then click Display.
   The Display dialog box is displayed.
- 2. Click the General tab, and use the following guidelines:



a. Select best display setting on DDC monitor—If the monitor is VESA DDC2B (Display Data Channel) compatible, selecting this option allows the thin client to automatically select the best resolution and refresh rate.

If your monitor is not DDC compatible, then **Monitor does not support Plug and Play** message is displayed. Click **OK** to acknowledge the message and remove it from the screen.

- b. **DDC table**—If the monitor is VESA DDC2B (Display Data Channel) compatible, selection of this option allows you to select the resolution and refresh rate you want from the list.
- c. User defined display setting—Select this option and select the resolution and refresh rate supported by your monitor. All combinations are allowed.

Resolutions include:

 $640 \times 480$  (Display resolution not supported on Wyse 3020 thin client with ThinOS—T10D)

800 x 600 (Display resolution not supported on Wyse 3020 thin client with ThinOS—T10D)

1024 x 768

1152 x 864

 $1280 \times 720$ 

1280 x 768 (Display resolution not supported on Wyse 3010 thin client with ThinOS—T10)

1280 x 1024

 $1360 \times 768$  (Display resolution not supported on Wyse 3010 thin client with ThinOS—T class)

1366 x 768

 $1368 \times 768$  (Display resolution not supported on Wyse 3010 thin client with ThinOS—T class)

1400 x 1050

1440 × 900

1600 × 900

1600 x 1200

1680 x 1050

1920 x 1080

1920 x 1200

1920 x 1440

2560 x 1080

2560 x 1440

2560 x 1600

3440 x 1440 (Display resolution supported on Wyse 3030 LT, 5010 and 5060 thin clients)

3840 x 2160

- d. Rotation—Select a rotation option. The available options are None, Left turn 90 degrees, or Right turn 90 degrees.
- e. **Desktop Color**—Only 32-bit is permitted. This value is selected by default. From ThinOS version 8.6 release, only 32-bit desktop color is supported on Wyse 3010 (T10) and 3020 (T10D) thin clients.
- f. **Usage Help**—This section contains brief instructions for using the **Display** dialog box and running the test. No operator entry can be made in this box.

Make note of the instructions in the area, regarding v-key reset usage if there is display failure.

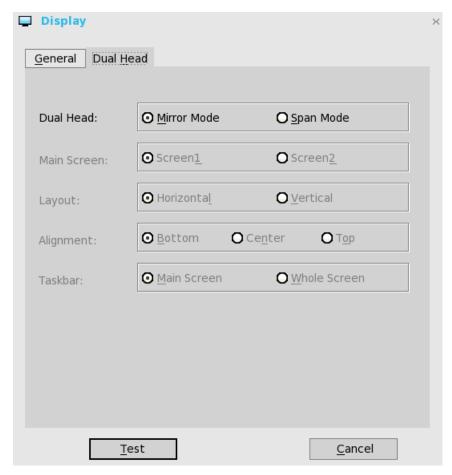
3. Click **OK** to save the settings.

For information about the tested monitors, see the latest Dell Wyse ThinOS Release Notes.

### Configuring the Dual Head display settings

This section is not applicable to Wyse 5070 thin client. To configure the Dual Head display settings:

- From the desktop menu, click System Setup, and then click Display.
   The Display dialog box is displayed.
- 2. Click **Dual Head** tab, and use the following guidelines:



This feature is applicable for supported Dual Monitor capable thin clients Only.

- a. Dual Head—Select Mirror Mode to have the two monitors work in a matching state, or Span Mode to have the two monitors work separately second is extended from first.
- b. Main Screen—Select which of the two monitors you want to be the main screen (Screen1 or Screen2). The other screen is extended from the main screen.

The other screen is extended from the main screen. When using a DVI to DVI/VGA splitter with VGA and DVI monitors at the same time, the VGA monitor will be the primary monitor.

c. Layout—Select how you want the two monitors to be oriented to each other.

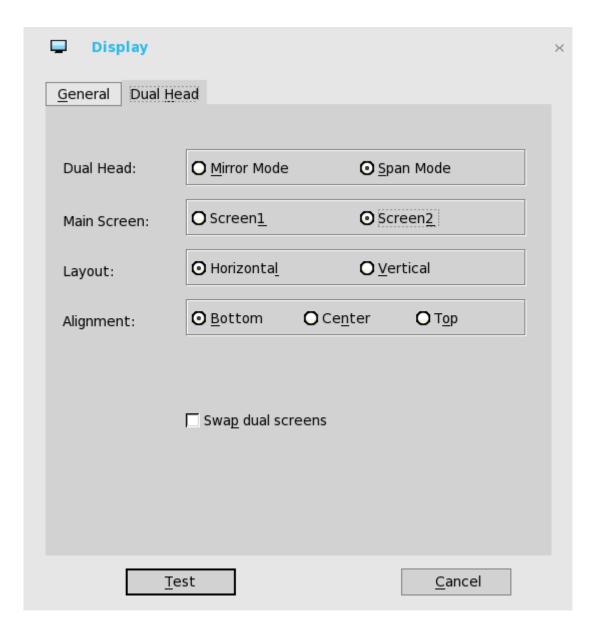
**Horizontal** — where you move between the monitors from the left and right of the screens.

**Vertical**— where you move between the monitors from the top and bottom of the screens.

d. Alignment— Select how you want the monitors to be aligned **Bottom**, **Center**, or **Top**.

Bottom means screens are bottom-aligned in a horizontal orientation; Center means screens are center-aligned; Top means screens are top-aligned in a horizontal orientation.

e. Taskbar (Classic Desktop Only)—Select under which screen you want the Taskbar to appear Whole Screen or Main Screen



For Swap dual screens, when you set Main Screen to Screen2, an additional check box is displayed at the bottom of the tab that allows you to swap dual screens. If you clear the check box, the Screen1 is usually the left one or the top one in dual display. When you set Main Screen to Screen2, the main screen is changed to the right screen or bottom screen. If you select the **swap dual screens** check box, you are able to set Main Screen to Screen2, but still have it at the left side or the top side, which is considered more user friendly.

### **Changing Display Settings Dynamically**

From ThinOS 8.4 release, after you change the display settings, the changes will take effect immediately without a system restart.

#### Single mode user scenario

Go to **System Setup** > **Display** > **General**, and do the following:

- 1. Change resolution from DDC table or User defined display settings.
- $\begin{tabular}{ll} \bf 2. & Change\ rotation\ setting\ from\ User\ defined\ display\ settings. \end{tabular}$

When the display settings are changed, the modified settings are applied to the active sessions dynamically. But some of the active sessions disconnect and then reconnect. For example, RDP for Win7 session.

### **Dual Head user scenario**

Go to **System Setup > Display > Dual Head** and change the settings.

Go to **System Setup** > **Display** > **General**, and do the following:

1. Change resolution from DDC table or User defined display settings.

2. Change rotation setting from User defined display settings.

When the display settings are changed during active sessions, the active sessions do not resize dynamically in the following situations:

- Seamless sessions
- · For dual head mode, including:
  - o Change from single mode to dual head.
  - o Change from dual head to single mode.
  - o Change display setting in dual head mode.

To apply the settings, disconnect the session and reconnect it.

### **Vertical Synchronization**

Vertical Synchronization or V-Sync enables the ThinOS client to synchronize the frame rate of a video with the monitor refresh rate to avoid screen tearing. Screen tearing occurs when the graphic processor delivers display frames more than your monitor can process. As a result, the image appears to be cut in half. Enabling VSync synchronizes the output video of the graphics card to the refresh rate of the monitor.

In ThinOS version 8.6, V-Sync is enabled by default. Vertical Synchronization feature is not supported on Wyse 3010, 3020, and 3030 LT thin clients.

#### Limitation

The ThinOS client desktop background flashes for a second when the RDP session desktop is connected with H.264- AVC444 enabled.

### **Dell Docking Station WD19**

The Wyse 5470 Thin Client supports the Dell Docking Station WD19. The Dell Docking Station WD19 is a device that links all your electronic devices to your thin client using a USB Type-C cable interface. Connecting the thin client to the docking station enables you to access all peripherals (mouse, keyboard, stereo speakers, external hard drive, and large-screen displays) without having to plug each one into the thin client.

ThinOS supports the Wake-on-LAN feature over the Dell Docking Station WD19 to wake up thin clients from sleep mode or the shutdown state. To use this feature, you must add the INI parameter wakeonusb=yes.

#### Limitations

- · USB Type-C and HDMI ports on Dell Docking Station WD19 are mutually exclusive.
- · Supports one Quad HD display at 30 Hz and two Full HD displays at 60 Hz.
- If two displays with resolution greater than 1920 x 1080 are connected simultaneously, only one display works. You must change the
  resolutions to 1920 x 1080 or lower to make both displays work.

#### Upgrade docking station firmware using ThinOS

You can update the Dell Docking Station WD19 firmware in a VDI session on ThinOS.

To upgrade the docking station firmware, do the following:

- 1. Connect the AC adapter to a power outlet. Then, connect the AC adapter to the 7.4 mm DC-in power input on the Dell Docking Station WD19.
- 2. Connect the USB Type-C connector to the thin client.
- 3. Launch a VDI session. By default, the dock is redirected to a VDI session.
- 4. Download the Dock Firmware Update Utility from www.dell.com/support.
- 5. Start the tool.
- 6. Wait for all the information to be entered in the various Graphical User Interface (GUI) panes.
- 7. Click the **Update** button.

For more information about the Docking Station, see the Dell Docking Station WD19 User's Guide at www.dell.com/manuals.

# Configuring the peripherals settings

The **Peripherals** dialog box enables you to configure the settings for the Keyboard, Mouse, Audio, Serial, Camera, Touch Screen, and Bluetooth.

## Configuring the keyboard settings

To configure the keyboard settings:

- 1. From the desktop menu, click **System Setup**, and then click **Peripherals**. The **Peripherals** dialog box is displayed.
- 2. Click the **Keyboard** tab and set the Character Set, Keyboard Layout, Delay Before Repeat and Repeat Rate parameters. The following table explains the keyboard parameters.

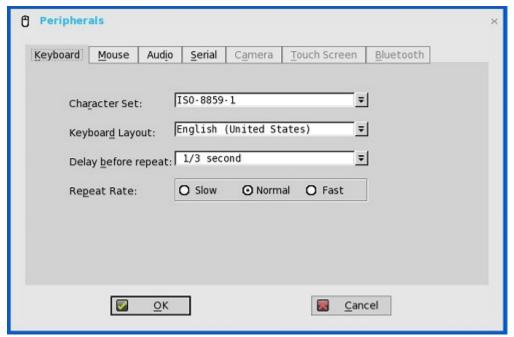


Table 38. Keyboard settings

Parameter	Description
Character Set	Specifies the character set. Each character is represented by a number. The ASCII character set, for example, uses the numbers 0 through 127 to represent all English characters and special control characters. European ISO character sets are similar to ASCII, but they contain additional characters for European languages.
Keyboard Layout	Presently the keyboard languages listed in the <b>Keyboard layout</b> drop-down list are supported. The default value is <b>English</b> (United States).
Delay Before Repeat	Specifies the repeat parameters for held-down key. Select the Delay before repeat value as either 1/5 second, 1/4 second, 1/3 second, 1/2 second, 3/4 second, 1 second, 2 seconds, or No Repeat. The default is 1/3 second.
Repeat Rate	Select <b>Slow</b> , <b>Normal</b> , or <b>Fast</b> . The default value is Medium.

3. Click **OK** to save the settings.

### **Function key combinations**

The Wyse 5470 Thin Client supports the following Function (Fn) key combinations:

i NOTE: Blast protocol does not support Fn keys.

#### Table 39. Fn key combinations

Key	ThinOS Local	VDI Session (RDP/ICA/PCoIP)
Fn + Esc	Fn lock/unlock	Function key lock or unlock

Table 39. Fn key combinations (continued)

Key	ThinOS Local	VDI Session (RDP/ICA/PCoIP)
Fn + F1	Mute	Mute
Fn + F2	Volume down	Volume down
Fn + F3	Volume up	Volume up
Fn + F4	Not applicable—session only	Previous file in Media Player list
Fn + F5	Not applicable—session only	Play or Pause in Media Player
Fn + F6	Not applicable—session only	Next file in Media Player list
Fn + F7	Not applicable	Not applicable
Fn + F8	Opens the Display Setup window	Not applicable—ThinOS local only
Fn + F9	Not applicable—session only	Opens the search window
Fn + F10	Keyboard light	Not applicable—ThinOS local only
Fn + F11	Screen dimming	Not applicable—ThinOS local only
Fn + F12	Screen lighting	Not applicable—ThinOS local only
Fn + Ctrl	Right-click mouse	Right-click mouse
Fn + PrtScr	Turn on/off wireless	Not applicable—ThinOS local only
Fn + Right arrow	Not applicable—session only	End
Fn + Left arrow	Not applicable—session only	Home
Fn + Up arrow	Not applicable—session only	Page up
Fn + Down arrow	Not applicable—session only	Page down

### (i) NOTE:

- If the Wi-Fi is turned on, pressing Fn + PrtScr disables the Wi-Fi on the thin client. The Disable Wireless Device check box and the Always option are selected in the Network Setup window.
- If the Wi-Fi is turned off, pressing Fn + PrtScr enables the Wi-Fi on the thin client. The Disable Wireless Device check box is cleared in the Network Setup window.

## Configuring the mouse settings

To configure the mouse settings:

- From the desktop menu, click System Setup, and then click Peripherals.
   The Peripherals dialog box is displayed.
- 2. Click the **Mouse** tab to select the mouse speed and mouse orientation.
  - NOTE: The mouse cursor speed can be increased up to 11 levels from ThinOS 8.6\_412 release. The cursor speed can be configured from the user interface or by using the INI parameters. However, in Wyse Management Suite the cursor speed can only be configured using advanced INI parameters.
- 3. Select the **Swap left and right mouse buttons** check box to swap mouse buttons for left-handed operations.
- 4. Select the Reverse mouse wheel scroll direction check box to invert the direction of the mouse scroll wheel.
- 5. Select the **Enable big mouse pointer** check box to increase the size of the local mouse pointer by two times.
  - NOTE: This option affects ThinOS local mouse pointer.
- 6. Select the **Disable trackpad** check box if you want to disable the touchpad on the device. This option is applicable only to the Wyse 5470 Thin Client.
- 7. Select the **Disable trackpad while typing** check box if you want to disable the touchpad while typing using the integrated keyboard. This option is applicable only to the Wyse 5470 Thin Client.
- 8. Click **OK** to save the settings.

#### **Touchpad gestures**

This section is applicable to the Wyse 5470 Thin Client.

The touchpad on the Wyse 5470 Thin Client contains two buttons for the right and left mouse-clicks. The following table lists the supported touchpad gestures on the Wyse 5470 Thin Client:

#### Table 40. Touchpad gestures

Touchpad gesture	Additional information
Moving the mouse cursor	Moving with one finger, the entire touchpad including the area with the buttons can be used for the mouse cursor movement.  i NOTE: The sensitivity of the cursor movement on the area with the buttons is slower compared to the other areas. This design is for the stability of the buttons.
Left-click	<ul> <li>Tapping with one finger anywhere on the touchpad works as the mouse left-click.</li> <li>Pressing the left button on the touchpad works as the mouse left-click.</li> </ul>
Right-click	<ul> <li>Tapping with two fingers anywhere on the touchpad works as the mouse right-click.</li> <li>Pressing the right button on the touchpad as the mouse right-click.</li> </ul>
Moving windows	<ul> <li>Press and hold the left button and move the window by dragging a second finger on the touchpad.</li> <li>Dragging a window by tapping twice on the touchpad with one finger is not supported.</li> </ul>

### Configuring the audio settings

To configure the audio settings:

- 1. From the desktop menu, click **System Setup**, and then click **Peripherals**.
  - The **Peripherals** dialog box is displayed.
- 2. Click the Audio tab to select the volume settings for connected devices.
  - a. Click the Playback Devices tab to select the type of the audio from the drop-down menu.
    - If the HD audio and DP audio options are available in playback devices, the thin client determines the priority between HD audio and DP audio when the DP cable is connected. In this scenario, select the playback device type that is based on your preference, and click **OK**. The playback device which you select takes the priority.
    - · Use **slider** to control the volume settings for the playback devices.
    - · Select the check box to mute.
  - b. Click the Recorded Devices tab to select the type of the record from the drop-down list.
    - · Use **slider** to control the volume settings for the record devices.
    - · Select the check box to mute.
  - c. Click Play to play the audio.
  - d. Use the Recorder tab and do the following:
    - · Collect information about the speaker and microphone being used.
    - · Examine the performance of the speaker and microphone being used.

For example, the connected USB headsets are displayed in the drop-down. Select the **HD audio** option for analog earphone use, the **Speaker** check box to enable the internal speaker, and the **Boost** check box for audio enhancement.

- e. Select the **Speaker** check box to connect the speaker.
- f. Select the **Boost** check box to boost the connected devices.
- g. Select the Enable DP audio check box to enable the DisplayPort audio function on your thin client. You must click either Port 1 or Port 2 to select your desired DisplayPort.

On the Wyse 5470 Thin Client, ThinOS supports DP audio only over one port. You must select either **Port 1** or **Port 2** based on your port preferences. On the Wyse 5470 All-in-One Thin Client, only **Port 1** is available.

h. Select the **Enable headset popup** check box if you want the headset popup dialog box to be displayed when you connect an analog headset to the front headset jack.

In the headset popup dialog box, select any one of the following audio devices:

- Headset
- · Headphone

- · Speaker
- NOTE: To disable the headset popup dialog box, select the Not show again check box, and click OK. You can also use an INI parameter to enable or disable the headset popup dialog box. For more information about INI parameters, see the latest *Dell Wyse ThinOS INI Reference Guide*.
- 3. Click OK to save your changes.

### **Using DisplayPort audio**

Use the DisplayPort (DP) interface to connect your thin clients to the display devices. The interface can include audio signals in the same cable as the video signals. To enable the DisplayPort audio, ensure that you set up the following components:

- · A thin client that supports DisplayPort audio and/or dual mode with audio.
- · A display device, such as monitor, that supports audio playback in ICA, RDP, Blast, or the PCoIP sessions.
- · An analog audio device or a monitor integrated speaker.

To enable the DisplayPort audio on ThinOS:

- 1. Set up a monitor with DP audio support.
- 2. Connect the ThinOS client to monitor using DP cable.
- 3. Plug the analog headset into the monitor DP audio interface.
- 4. On the ThinOS desktop, click System Setup > Peripherals > Audio > Playback devices, and select the Enable DP audio check box.
- 5. In the Audio tab. select either Port 1 or Port 2.
- 6. Start either an RDP, ICA, PCoIP, or Blast session.
- 7. Play a video, and check the audio output using the analog headset.

#### Limitations

- · ThinOS supports only the DisplayPort audio playback. Audio recording using DisplayPort is not supported.
- · DisplayPort audio is supported only on Wyse 3030 LT thin client, Wyse 5060 thin client, and Wyse 5070 thin client.
- By default, the DP audio is disabled on Wyse 3040 thin client. If you update ThinOS to a newer version, the default setting for DP audio is not set automatically. You must reset the thin client to factory default settings to load the default settings for DP audio. However, thin clients shipped with the latest version of ThinOS are already configured with default settings.

If you enable the DP audio, and select the DP audio as the playback device, the following issues are observed:

- o A black screen is displayed for a few seconds during the system reboot.
- o DP audio stops responding, and a black screen is displayed when you play an audio file.

#### Limitations on the Wyse 5470 Thin Client

- · You must enable the DP audio as it is disabled by default.
- HDMI, DisplayPort over USB Type-C port, and USB Type-C port audio is displayed as DP audio.
- · Hot plugging is not supported. You must plug in the HDMI cable, USB Type-C cable, or the DP cable, and reboot the thin client for the DP audio to work.
- · Converter is not supported.
- · Supports only audio over the integrated HDMI port with selected displays.
- DP audio works when you connect a single DP audio supported display to the thin client through the WD19 docking station. If you connect two DP audio supported displays to the thin client through the WD19 docking station, DP audio does not work.
- Turning off or turning on the display is not supported. Restart the thin client for the DP audio to work in the following scenarios:
  - $\circ\quad$  If the power button is pressed, to power off, and then power on the display.
  - o If the screen saver is set to Turn Off Screen.
  - o If you click **Apply** on the **Display setup** window.

#### Limitations on the Wyse 5470 All-in-One Thin Client

- · You must enable the DP audio as it is disabled by default.
- · Hot plugging is not supported. You must plug in the DP cable, and reboot the thin client for the DP audio to work.
- · Converter is not supported.
- · Turning off or turning on the display is not supported. Restart the thin client for the DP audio to work in the following scenarios:
  - o If the power button is pressed, to power off, and then power on the display.
  - o If the screen saver is set to **Turn Off Screen**.
  - o If you click **Apply** on the **Display setup** window.

### **Using PulseAudio**

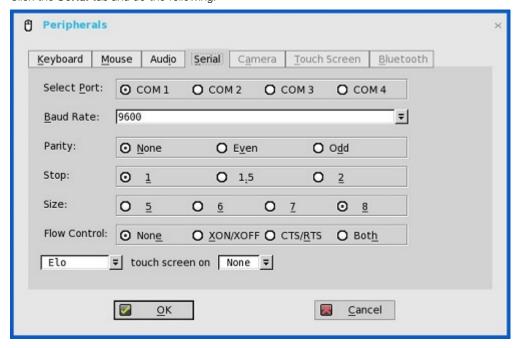
PulseAudio is a sound server that runs on ThinOS to deliver audio and manage audio devices. PulseAudio supports multiple audio devices when using real-time audio applications in ICA, RTME, and other VDI sessions.

i NOTE: You cannot disable the PulseAudio feature on your ThinOS client.

### Configuring the serial settings

To configure the Serial settings:

- From the desktop menu, click System Setup, and then click Peripherals.
   The Peripherals dialog box is displayed.
- 2. Click the Serial tab and do the following:



- a. Select Port—Click the button to select the Port. Default is COM 1.
- b. Baud Rate—Select the Baud Rate from the drop-down list. Default is 9600.
- c. Parity—Click the button to select the Parity.
- d. Stop—Click the button to select the stop bits 1, 1.5, 2. Default value is 1.
- e. Size—Click the button to select the Character size 5, 6, 7, or 8 bits. Default is 8.
- f. Flow Control—Click the button to select Flow Control: Either None, XON/XOFF, CTS/RTS, or Both can be selected. Default is None.
- g. Serial Touch Screen selections—Select the required touch screen from the drop-down list. Available options are ELO, MicroTouch and FastPoint.
- h. Touch Screen on—Select the required serial port (COM port) or None from the drop-down list.
- 3. Click **OK** to save the settings.

ThinOS enables you to disable the onboard serial port on the following platforms:

- · Wyse 5070 Thin Client with Celeron processor
- · Wyse 5070 Thin Client with Pentium processor
- · Wyse 5070 Extended Thin Client with Pentium processor

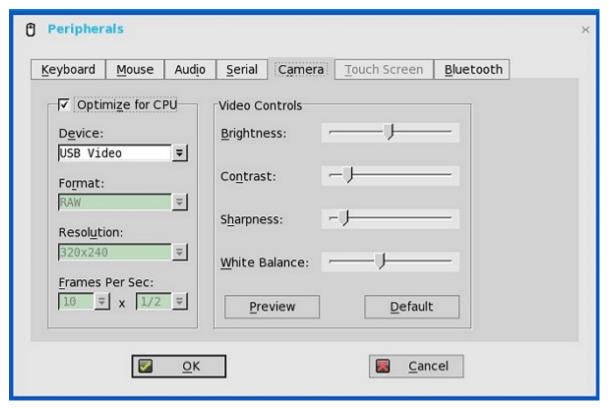
To disable or enable the onboard serial port, use the INI parameter *Device=SerialDisable={yes, no}*. The default value is no. This option does not affect the USB serial devices. The value that you specify is saved into NVRAM and a system reboot is required for changes to take effect.

After the onboard port is disabled, all the port values—COM1, COM2, COM3, and COM4—are available for USB serial device mapping. You can view the ThinOS event log to know the local serial port name that is used when a USB serial device is attached to the thin client.

### Configuring the camera settings

Use the **Camera** tab to interface with cameras that are locally connected to the thin client (USB) and supported by a UVC driver. When using the HDX RealTime webcam feature of Citrix Virtual Apps and Desktops, you can control options such as maximum resolution and frames per second (10 FPS is recommended).

By default, the format of USB camera is set to RAW.



### (i) NOTE:

You can optimize performance and modify the frame rate per second, if the Optimize for CPU check box is not selected —supported values include 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6- directly from the thin client (if the webcam supports Universal Video Driver).

Also, this feature is CPU intensive and is recommended for high performance products.

For Wyse 5470 and Wyse 5470 All-in-One thin clients, it is recommended to use a camera such as Logitech C930e that supports hardware encoding. The integrated camera on the thin clients does not support hardware encoding, so the performance is limited as follows:

- On the Wyse 5470 Thin Client with RTME-enabled, the camera performance on Skype for Business is limited to a maximum resolution of 640 x 360 using HD configuration, 960 x 540 using Full HD configuration, and 1280 x 720 if Logitech C930e camera is used.
- On the Wyse 5470 All-in-One Thin Client with RTME-enabled, the camera performance on Skype for Business is limited to a maximum resolution of 960 x 540, and 1280 x 720 if Logitech C930e camera is used.
- On a JVDI-enabled client, the CPU usage of the integrated camera is 10% higher than the CPU usage of Logitech C930e camera. The difference in the CPU usage is observed while video calling on Cisco Jabber in a ICA session.

### Configuring the touch screen settings

Use the **Touch Screen** tab to configure touch screens that are connected to the thin client. The tab is available (not grayed out) when the thin client detects that a touch screen is attached through a USB port or a serial port, and the setup or calibration has not been performed. The Touch Setup window prompts you to touch two circles on the screen to make the necessary calibration adjustment. The adjusted calibrated values are saved in the local terminal NVRAM until the system is reset to factory default, or another type of touch monitor is connected.

NOTE: From ThinOS version 8.5, the ELO touch screen does not work in certain scenarios. For more information, see the latest Dell Wyse ThinOS Release Notes.

Touch screen is an optional configuration for the Wyse 5470 Thin Client. It is recommended to use the default 1920 x 1080 resolution while using touch screen. If you use a custom resolution, the touch screen does not calibrate accurately.

### Configure the touch screen settings for VDI sessions

When you connect a touch monitor to the client using USB port, you must change the configurations in Global Connection Settings.

### **Configure touch monitor for RDP Session**

- 1. From the desktop menu, click Connect Manager.
- 2. Click Global Connection Settings.
- 3. Select the USB devices redirection check box and configure the following options:
  - a. Clear the Exclude disk devices check box.
  - b. Select the Exclude printer devices check box.
  - c. Select the Exclude audio devices check box.
  - d. Select the Exclude video devices check box.

#### Configure touch monitor for Citrix and VMware Sessions

- 1. From the desktop menu, click Connect Manager.
- 2. Click Global Connection Settings.
- 3. Select the **USB devices redirection** check box and configure the following options:
  - a. Clear the Exclude disk devices check box.
  - b. Clear the Exclude printer devices check box.
  - c. Clear the Exclude audio devices check box.
  - d. Clear the Exclude video devices check box.

### Configuring the Bluetooth settings

The Bluetooth feature helps you to connect your thin client with Bluetooth enabled devices such as headsets and mouses.

ThinOS supports both Intel wireless chipset 7260 and 7265.

ThinOS supports Intel Dual Band Wireless AC 9560 chipset on Wyse 5070 thin client.

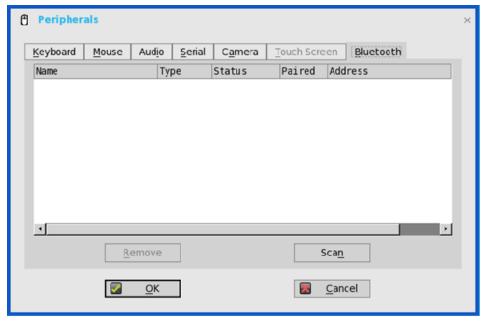
For mouse, keyboard, and headset, ThinOS supports both Bluetooth 3.0 and 4.0.

Bluetooth 4.0 supports Classic and Bluetooth Low Energy (BLE). However, Bluetooth Alternate MAC/PHY (AMP) is not supported.

NOTE: From ThinOS v8.4.1, the Bluetooth feature is supported on Wyse 3040 thin client with ThinOS and Wyse 3040 thin client with PCoIP.

To configure the Bluetooth settings:

From the desktop menu, click System Setup, and then click Peripherals.
 The Peripherals dialog box is displayed.



2. Click the **Bluetooth** tab, and use the following guidelines:

Bluetooth enabled devices, such as headsets and mouses that are available in the thin client environment are listed in the **Bluetooth** page. The following attributes are displayed in the list:

- · Name—Specifies the name of the Bluetooth enabled device.
- · Type—Specifies the type of the Bluetooth enabled devices, such as headsets, mouses, and keyboards.

Both Human Interface Devices (HID) and Headset Bluetooth devices are supported.

- o **HID** type
  - HID includes mouse and keyboard.
  - The maximum number of HIDs that can be connected is seven.
- Headset type
  - The Bluetooth headset is supported in this release.
  - The maximum number of Bluetooth headsets that can be connected is one.
- NOTE: Other types of Bluetooth devices are not scanned and supported. Call level audio quality on headsets is supported. However, multimedia are still not supported.
- · Status—The Bluetooth page has two columns, namely, Status and Paired.

Table 41. Bluetooth status

Attribute	Value	Summary
Status	Connected	The Bluetooth device is connected to the ThinOS device. It is ready to be used.
	Connecting	The Bluetooth device is connecting to the ThinOS device.
	Disconnected	The Bluetooth device is not connected to the ThinOS device.
Paired	Yes	The Bluetooth device is paired with the ThinOS device.
	No	The Bluetooth device is not paired with the ThinOS device.

• Address—Displays the address of the Bluetooth device connected to your thin client.

The following are the user scenarios and corresponding Bluetooth statuses displayed on the Bluetooth page:

#### Table 42. User scenario

User scenario	Status
Device turned off	Disconnected   Paired
Device turned on	Connected   Paired
Device disconnected from ThinOS	Disconnected   Not Paired

- Scan—All Bluetooth devices enter into Page Scan mode. Different Bluetooth devices enter into the Page Scan mode at different instances such as when a specific button is pressed three times or a specific button is pressed and held until the LED turns blue.
- Connect—Select a particular Bluetooth enabled device, and click Connect to connect the selected device to the thin client. If
  the Bluetooth device is connected successfully, the status is displayed as Connected in the Bluetooth window.
- · Remove—Select a particular Bluetooth device, and click Remove to disconnect and remove the device from the list.
- Auto Connect function—The Auto Connect function is designed for HIDs.
  - o ThinOS has no HIDs connected such as USB or Bluetooth HIDs.
  - The Bluetooth HIDs are configured as Page Scan mode.

When you start the ThinOS client, the Bluetooth HIDs can connect to ThinOS automatically without scanning or pairing operations. The Bluetooth HIDs automatically reconnect after you restart the ThinOS client.

· Reconnect function—The Reconnect function is designed for HIDs and headsets.

When you restart the system with the Bluetooth device (HID/headset) that is already paired and connected, the Bluetooth device automatically reconnects within a few seconds.

For example, you can hover the Bluetooth mouse, and then click a few times for the Bluetooth mouse to reconnect successfully. The Bluetooth headset reconnects automatically, but might require you to manually close or reopen the device on certain occasions.

To know about the certified devices and known issues, see the latest Dell Wyse ThinOS release notes at www.dell.com/support.

### **USB** support

**USB port**—Wyse 7010 with ThinOS (Z10D) supports two USB 3.0 ports. USB 3.0 is compatible with USB 2.0. When USB 2.0 device is connected to 3.0 ports, the behavior of the device remains unaltered. For USB 3.0 device to connect to 3.0 ports, the device type should be of 5 Gbps. All types of USB devices work when connected to USB 3.0 port.

**USB hard disk**—Do not plug in the USB hard disk with 10 or more drives, or do not plug in more than 10 USB keys into ThinOS client. ThinOS does not detect the USB disk with 10 or more drives.

Known issue—Camera preview has some known issue.

### Support for USB Type-C

Wyse 5070 thin client supports the USB Type-C port.

- The USB 3.1 Type-C connector can be used to perform the following activities:
  - o Transfer data by using USB mass storage
  - Connect monitors
    - NOTE: If you use USB Type-C, one monitor capability is reduced from rear panel, and DP2 is disabled.
  - o Charge smartphones
  - o Connect USB 2.0, 3.0, and 3.1 compatible devices.
- · The USB 3.1 Type-C cannot be used for the following:
  - Thunderbolt, HDMI, and MHL alt modes
  - o Docking stations
  - o Powering a thin client
- Limitation—In Wyse 5070 thin client, XHCI is used for all types of USB devices. The transmission speed gap between USB 3.0 and USB Type-C is not significant.

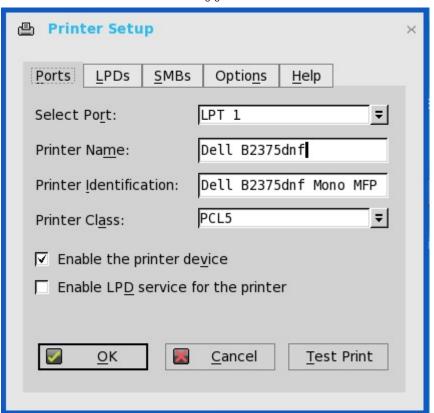
# Configuring the printer settings

Use the **Printer Setup** dialog box to configure network printers and local printers that are connected to the thin client. Through its USB ports, a thin client can support multiple printers. If more than one printer is to be used and another port is not available on your thin client and the port that is to be used must be shared with a USB modem converter, connect a USB hub to the port.

### Configuring the ports settings

To configure the ports settings:

- From the desktop menu, click System Setup, and then click Printer.
   The Printer Setup dialog box is displayed.
- 2. Click the Ports tab, and use the following guidelines:



- a. Select Port Select the port you want from the list. LPT1 or LPT2 selects the connection to a direct-connected USB printer.
- b. Printer Name (Required) Enter name you want displayed in your list of printers.
  - most USB direct-connected printers report/fill in their printer name automatically.
  - NOTE: If Enable LPD service for the printer is selected, the printer name becomes the queue name for other clients using LPR to print to this printer.
- c. **Printer Identification** Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces, most USB direct-connected printers report/fill in their printer identifications automatically.

This entry must be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or **Generic / Text Only** for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

NOTE: The maximum characters allowed in the Printer Identification field is 31. If your printer driver string is more than 31 characters (including space), you can create a txt file (printer.txt) and upload to your file server.

Edit the txt file and type the content, such as "HP Color" = "HP Color LaserJet CM1312 MFP PCL6

Class Driver". Add the command line printermap=printer.txt to your wnos.ini file. Now, you can type "HP Color" in the Printer Identification field instead of the full driver string.

- d. Printer Class— This is optional. Select the printer class from the list PCL5, PS, or TXT or PCL4.
- e. Enable the printer device Select this option to enable the directly-connected printer. It enables the device to display on the remote host.
- f. Enable LPD service for the printer Select this to make the thin client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network.
  - (i) NOTE:

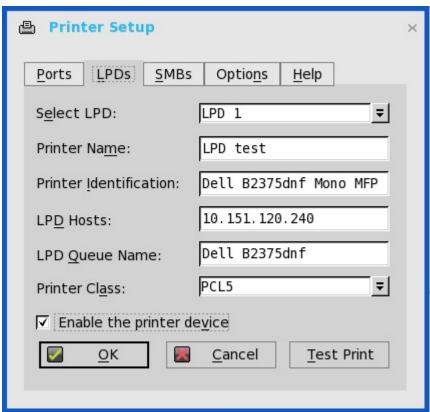
If the thin client is to be used as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the client, see Configuring the Network Settings.

3. Click **OK** to save the settings.

### Configuring the LPDs settings

To configure the LPDs settings:

- From the desktop menu, click System Setup, and then click Printer.
   The Printer Setup dialog box is displayed.
- 2. Click the LPDs tab, and use the following guidelines when printing to a non-Windows network printer:



- i NOTE: Be sure to check with your vendor that the printer can accept Line Printer Request print requests.
- a. Select LPD —Select the port you want from the list.
- b. **Printer Name** (Required) Enter name you want displayed in your list of printers.
- c. **Printer Identification**—Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

This name must be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or **Generic / Text** for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

d. LPD Hosts—The DNS or WINS name of the server for the network printer. An IP address of the printer on the network can also be entered.

If the printer is attached to another thin client on your network, the entry in the LPD Hosts box is the name or address of that thin client.

e. LPD Queue Name—An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer to be used.

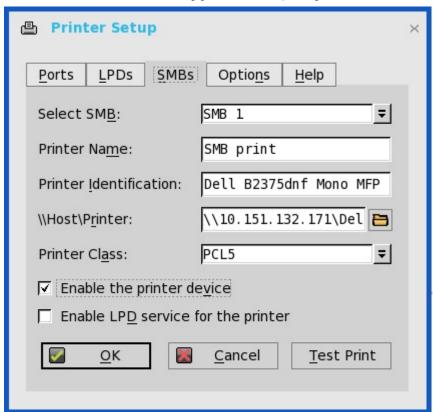
This name can be different for each vendor. This field is required and must be correct so that the network printer accepts incoming print jobs properly. For example, auto can be used for HP LaserJet 4200n PCL6 as per documentation found on the HP Web site.

- NOTE: If the printer is attached to another thin client on your network, the LPD Queue Name must match the content of the Printer Name box on the thin client with the printer attached.
- f. Printer Class— (Optional) Select the printer class from the list.
- g. Enable the printer device—Must be selected to enable the printer. It enables the device so it displays on the remote host.
- 3. Click **OK** to save the settings.
  - NOTE: When the LPD printer is mapped to one session and you cannot access the LPD service host, then the TCP connection tries to connect to the LPD service host. The timeout period is 60 seconds. During this timeout period, if you try to close the session, the session waits until the LPD printer connection is established. The initialization failure logs are displayed.

# Configuring the SMBs settings

To configure the SMBs settings:

- From the desktop menu, click System Setup, and then click Printer.
   The Printer Setup dialog box is displayed.
- 2. Click SMBs tab, and use the following guidelines when printing to a Windows network printer.



- a. **Select SMB**—Select the SMB you want from the list.
- **b. Printer Name**—(Required) Enter the name to be displayed in your list of printers.
- c. **Printer Identification**—Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

This name must be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB

printers or **Generic / Text** for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

- d. \\Host\Printer—Enter the Host\Printer or use the browse folder icon next to the box to browse your Microsoft Networks and make the printer selection you want from the network printers available (the DNS name or IP address of the Windows print server on the network).
- e. Printer Class (Optional) Select the printer class from the list.
- f. Enable the printer device—Must be selected to enable the printer. It enables the device so it displays on the remote host.
- g. Enable LPD service for the printer—Select this to make the thin client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network, see Using Your Thin Client as a Print Server (LPD).

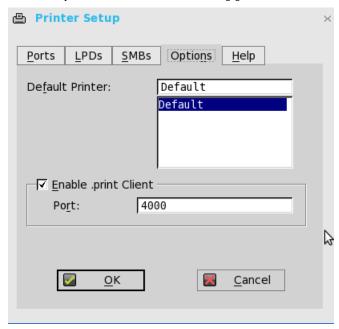
If the thin client is to be used as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the thin client as described in Configuring the Network Settings.

3. Click **OK** to save the settings.

## Using the printer setup options

To configure the printer setup options:

- From the desktop menu, click System Setup, and then click Printer.
   The Printer Setup dialog box is displayed.
- 2. Click the **Options** tab, and use the following guidelines:



- a. Default Printer Select the printer you want to be the default printer from your list of available printers.
- b. Enable .print Client and Port —If you want to enable .print Client, select Enable .print Client , and then enter the port.
- 3. Click **OK** to save the settings.

### **Using the Help**

When you click the Help tab, the following message is displayed in the text box.

Printer Identification is supplied by printer device. Change it to a Window's printer driver name or setup a driver mapping file.

## Reset features

Reset features include:

- · Resetting to factory defaults using G-Key reset
- · Resetting to factory defaults using shutdown reset
- Resetting display settings using V-Key reset

## Resetting to factory defaults using G-Key reset

High-privileged or stand-alone users can reset the thin client to factory default settings using the G-key reset feature.

To reset the thin client to factory default settings, restart the thin client and continuously tap the  $\bf G$  key during the restart process. G-key reset impacts all configuration items, including, but not limited to, both network configuration and connections defined in local NV-RAM.

i NOTE: G-key reset is disabled for Low-privileged and Non-privileged users in Lock down mode.

## Resetting to factory defaults using shutdown reset

A high-privileged or stand-alone user can reset the thin client to factory default settings from the **Shutdown** dialog box.

To reset the thin client to factory defaults:

- 1. From the desktop menu, click **Shutdown**. The **Shutdown** dialog box is displayed.
- 2. After starting your thin client you will see a **Dell logo** for a short period of time.
- 3. Click **Restart the system** to restart your thin client.
- 4. Select the **Reset the system setting to factory default** check box to restore your system settings to default factory settings.
- 5. Click **OK** to save the settings.

Shutdown reset impacts all configuration items, including, but not limited to network configuration and connections defined in local NV-RAM. However, the terminal name will not be changed.



Shutdown reset is disabled for Low-privileged and Non-privileged users, regardless of lock down state.

## Resetting display settings using V-Key reset

If the display settings are inappropriate for the particular monitor that is connected, it is possible that the display will not function properly when the thin client restarts. To correct this, power-on the thin client while continuously tapping the  $\boldsymbol{V}$  key. This will restart the thin client with a default/automatic display resolution.

## **TCX Suite**

#### (i) NOTE: TCX is not supported anymore as it is deprecated from the ThinOS 8.6\_303 release onwards.

Dell Wyse TCX Suite is a single software solution that provides the benefits of cloud client computing. The supported environments for Dell Wyse TCX Suite are Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, Citrix Virtual Apps, Teradici, and VMware Horizon View. The Collaborative Processing Architecture (CPA) used in Dell Wyse TCX divides the workload between the server and Plugn-Play USB devices. TCX Suite uses the established software protocols to provide breakthrough multimedia and audio technology for cloud client computing environments. For more information about the TCX features, see the latest *Dell Wyse TCX Administrator's Guide*.

TCX Suite enables rich flash playback, multiple monitors awareness, rich multimedia playback, high-quality bidirectional audio capabilities, and seamless USB device access for cloud clients.

TCX Suite provides the following features:

- TCX Flash Acceleration and TCX Flash Redirection—Enhances the performance of the Flash video content in a remote
  computing environment.
- TCX Multidisplay—Provides productivity, enhancing advantages for cloud clients with multiple monitors by using virtual desktops.
- TCX Multimedia—Supports enhanced playback of MPEG, WAV, WMV, H.264, and other multimedia file formats. The software includes both the server and the client components that redirect multimedia processing tasks between the client and server for a rich user experience.
- **TCX Rich Sound**—Provides bidirectional audio capabilities for virtual desktops and applications and supports sound recording and playback applications. It supports zero-compromise deployment.
- TCX USB Virtualizer—Makes the USB devices attached to thin clients or endpoints visible to the virtual desktops and applications. It removes any dependencies on limited local device drivers for a broad range of USB-based printers, scanners, storage devices, Palmtop, BlackBerry, Pocket PC handhelds, HID devices, Webcams, headsets, iPhone, credit card machines, and smart cards.
- · TCX Monitor—Helps you to efficiently identify the system state for proper functioning of USB and Flash Redirection modules.

#### **TCX Flash Redirection**

TCX Flash Redirection uses the client CPU to decode and render flash. TCX Flash Redirection uses the Adobe flash player plug-in that supports the NPAPI interface on the client. TCX Flash Redirection is supported over RDP and PCoIP protocols. TCX Flash Redirection uses less Server CPU cycles.

#### **Prerequisites**

- TCX.i386.pkg must be installed on client for the feature to work.
- TFRSServerBHO Class must be enabled in browser add-on.
- **Enable Protected Mode** is turned off in the Security options of Internet Explorer.
- Enable third-party browser extensions is enabled in the Advanced options of Internet Explorer.

#### Verifying the working status of TCX Flash Redirection

Verifying the status of TCX Flash Redirection is similar to HDX FR.

Use the following INI parameter to display the HW label:

MMRConfig=VIDEO flashingHW=1

NOTE: TCX FR on ThinOS is not working for certain flash video pages. However, the result is the same between FR over RDP, and FR over PCoIP. Dell recommends you to validate, and block the URL that does not work, before deploying TCX FR on all the systems.

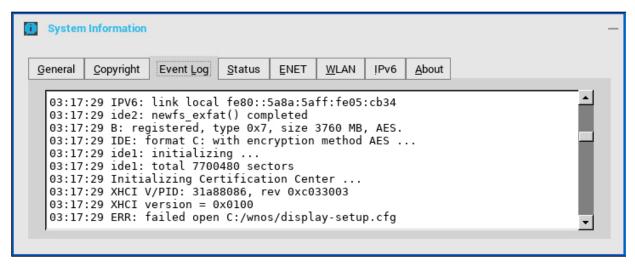
## **Trusted Platform Module version 2.0**

Wyse 5070 thin client supports disk encryption and decryption through Trusted Platform Module (TPM) version 2.0.

- Measured boot—SHA1 (Secure Hash Algorithm 1) is used to produce a hash value for ThinOS image, and extend the integrity
  measurement into Platform Configuration Registers (PCR) inside TPM—TPM\_PCR16. This is used to generate disk encryption or
  decryption key.
- · Disk encryption/decryption key
  - Disk C with user data and Disk B with system libraries are encrypted.
  - Prestored **KeyStub** and **TPM\_PCR16** are used to generate disk encryption and decryption keys through TPM. The actual implementation is based on TPM-unseal operation.
  - If the key is modified, the key fails to verify the specific disk partition. The disk partition is formatted to make the partition valid.
     The following screenshot displays the event log:

```
System Information
 General
          Copyright
                     Event Log
                                Status
                                        ENET
                                                WLAN
                                                              About
   03:17:29 TPM vendor: fc, rev: 1, capbilities 0x3000069f
   03:17:29 TSS unseal data: failed, rc 00000284
   03:17:29 TPM_RC_VALUE - value is out of range or is not correct for the conte
   xt Handle number 2
   03:17:29 IDE: format B: with encryption method AES ...
   03:17:29 ide5: initializing ...
   03:17:29 ide5: total 1048576 sectors
   03:17:29 ide2: initializing ...
03:17:29 IPV6: link local fe80::5a8a:5aff:fe05:cb34
   03:17:29 ide2: newfs_exfat() completed
```

Figure 37. Event log tab



#### Figure 38. Event log tab

After the disk partition is formatted, some user configurations, such as display settings, user certificates, wireless settings—except
the first SSID, as it is saved in NVRAM—cookie, and mirror file server data, are lost.

## **Performing diagnostics**

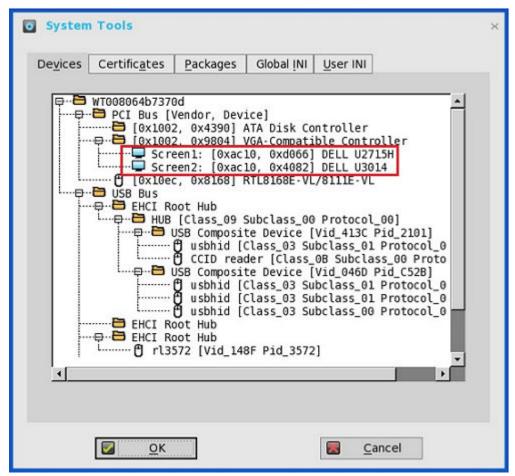
This chapter helps you identify and troubleshoot your thin client using the troubleshooting options.

## System tools

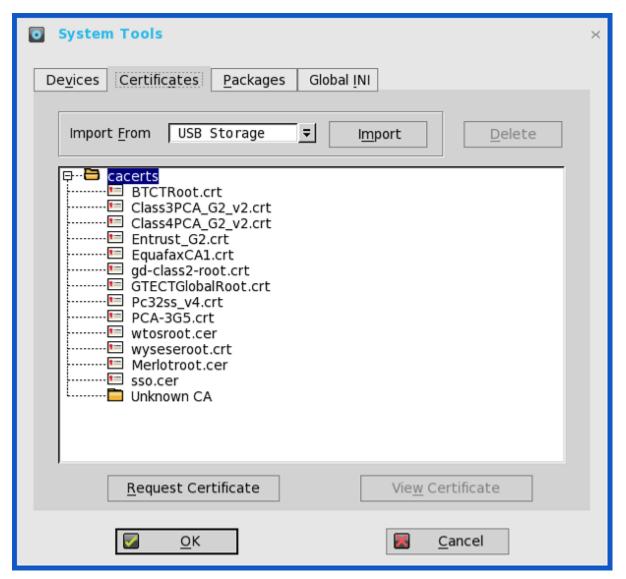
Use the **System Tools** dialog box to view device details, package details and Global INI/User INI information. You can also import certificates using the **Certificates** tab.

- From the desktop menu, click System Tools.
   The System Tools dialog box is displayed.
- 2. Click the **Devices** tab to display all the locally attached devices, including USB, Serial, and Parallel on applicable platforms. The details about the monitors connected to the thin client are also displayed.

The Device Viewer button was previously available in the **Devices** tab of the **System Information** dialog box.



- NOTE: The Mirror File Server tab has been removed from the System Tools dialog box, as it can now be viewed in the Devices tab.
- 3. Click the **Certificates** tab, and use the following guidelines:



- **a.** Import the certificates by selecting either USB Storage or File Server from the drop-down list, and then click **Import** to import the required certificate.
- b. Click **Delete** to delete the imported certificate.
- c. Click **View Certificate** to view the imported certificate information such as Version, Validity, and Serial number. You can also view the certificate path and certificate status. For more information about the default certificates, see About default certificates.
- d. Click **Request Certificate** to manually request certificate for your client. For more information about Simplified Certificate Enrollment Protocol, see Simplified Certificate Enrollment Protocol.
- 4. Click the Packages tab, and use the following guidelines:

ThinOS packages that are installed on thin client are listed in the **Packages** tab.

- a. Click the **Delete** button to delete the selected package.
- b. Click the **Delete all** button to delete all the packages.

The following packages are displayed in the **Package** tab:

- · base.i386.pkg
- FR.i386.pkg—This package is introduced to support Flash Redirection.
- RTME.i386.pkg—This package is introduced to support Citrix RTME.
- Horizon.i386.pkg—This package is introduced to support VMware Blast protocol. The package version number is updated to
  match the latest Horizon client.

To install this package, PKG installation INI file needs to be changed to AddPkg="horizon".

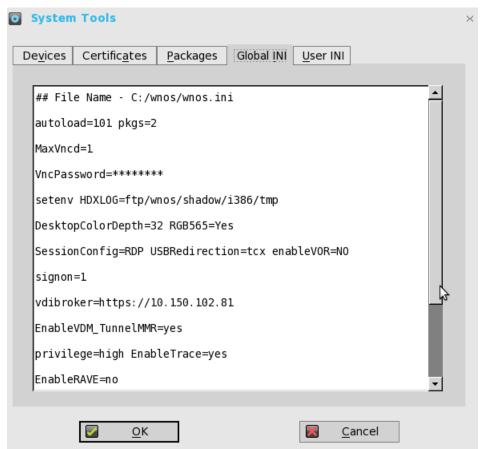
- · JVDI.i386.pkg—This package is introduced to support Cisco Jabber.
- pcoip.i386.pkg—This package is available only on Wyse 3030 LT with PCoIP, Wyse 3040 with PCoIP, Wyse 5010 with PCoIP (D10DP), Wyse 5040 AIO with PCoIP (5213), and Wyse 5060 with PCoIP.

• TCX.i386.pkg—This package is introduced to support TCX.

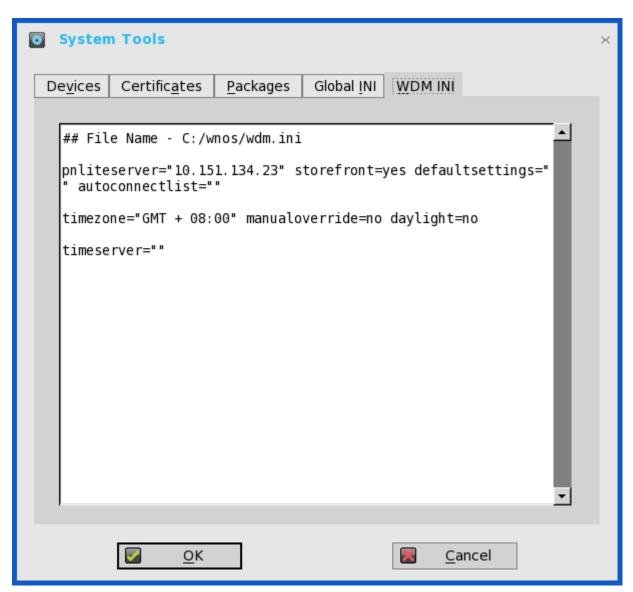
You cannot delete the base package separately. If you click **Delete All**, all packages are deleted including the base package. When you click **Delete All**, a message is displayed prompting you to restart the device.

The base.i386.pkg is mandatory for all ThinOS clients. At present, PCoIP package is mandatory for the PCoIP enabled thin clients. Other packages are optional. Base package and PCoIP package are integrated into the ThinOS firmware image. Installing the latest ThinOS firmware image will automatically install the latest version of these packages on ThinOS client. You cannot manually install or upgrade these embedded packages. However, the package version details of respective packages are displayed in the **Packages** tab for engineering information purpose only.

- NOTE: When you install packages or restart the ThinOS device, the ThinOS client verifies the version of the installed package. If you have not installed the latest package version, the details about the current package version and the recommended package version are displayed in the Event Log tab. In every ThinOS release, the packages may be updated to the latest version. For information about the latest package version, see the latest *Dell Wyse ThinOS release notes*.
- 5. Click the Global INI tab to view the wnos.ini information.



- 6. Click the User INI tab to view wnos.ini information.
- 7. Click the **WDM INI** to view the received WCM configurations.



WCM function is supported from WDM for comprehensive client configuration. Without configuration from server, the client loads the cached settings (wdm.ini), if available.

#### Limitation

To upgrade or downgrade firmware/image through WCM, you are required to enable WDM file server function by selecting the **WTOS INI path upon checkin (HTTPS/CIFS)** check box in the WTOS preferences in the WDM configuration manager.

8. Click **OK** to save the settings.

## **Simplified Certificate Enrollment Protocol**

Simplified Certificate Enrollment Protocol (SCEP) was used in a closed network where all end-points are trusted. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner. Within an enterprise domain, it enables network devices that do not run with domain credentials to enroll for certificates from a Certification Authority (CA).

At the end of the transactions that are defined in this protocol, the network device has a private key and associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

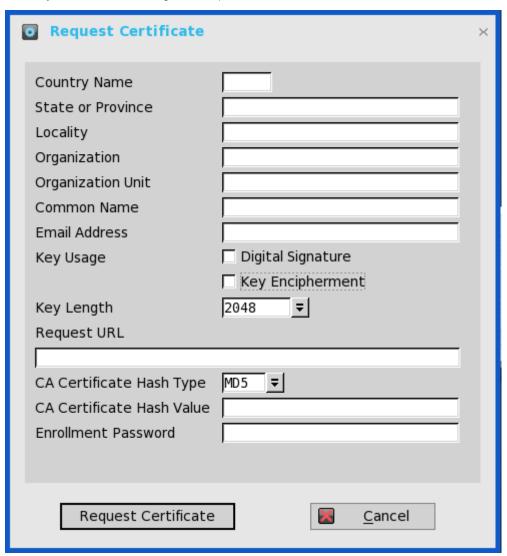
ThinOS is treated as a network device. The functionality of ThinOS SCEP includes manual certificate request, automatic certificate request, and automatic renewal of certificate.

## Requesting certificate manually

To request the certificate manually, do the following:

1. Go to System Tools > Certificates > Request Certificate.

The **Request Certificate** dialog box is displayed.



2. Enter the appropriate values in the Request Certificate dialog box, and then click the Request Certificate button.

The certificate request is sent to the server, and the client receives the response from server and installs both CA certificate and client certificate.

3. Click Ok to save the changes.

### (i) NOTE:

- The CA Certificate Hash type currently supports MD5, SHA1, and SHA256.
- The request server URL can be an HTTP or HTTPs link. You can add the protocol prefix before the URL.

### Requesting certificate automatically

Use INI parameters to automate the request, and renew the certificate process. Related INI parameters are of global scope and should be used with INI parameter ScepAutoEnroll.

For more information about using the INI parameters, refer to the latest Dell Wyse ThinOS INI Reference guide.

## **About Default Certificates**

Default certificates embedded in the ThinOS are displayed in the **Certificate** dialog box. To view the default certificate, set ThinOS to factory default, and on the desktop click **System Settings** > **System Tools** > **Certificates**. The following default certificates are displayed in the **cacerts** folder, in an expandable tree structure format:

- · BTCTRoot.crt
- · Class3PA G2 v2.crt
- · Class4PA\_G2\_v2.crt
- · Entrust G2.crt
- · EquafaxCA1.crt
- · gd-class2-root.crt
- · GTECTGlobalRoot.crt
- · Pc32ss\_v4.crt
- · PCA-3G5.crt

To view each certificate, select the certificate you want to view, and then click **View Certificate**. In the **Certificate** dialog box, click any of the following tabs to view the corresponding certificate attributes:

- 1. **General**—The following values are displayed:
  - · Purpose of the certificate
  - · Certificate issued to
  - · Certificate issued by
  - · Certificate valid period
- 2. **Details**—The certificate details are listed along with the corresponding default values. For information about individual certificates, see the **Certificate Details** section.
- 3. Certification Path—The folder path where the certificate is stored is displayed. Certificate status can be viewed in the lower pane of the window.

#### **Certificate details**

This section lists the certificates with the valid attributes and corresponding default values.

Certificate name—BTCTRoot.crt

Table 43. BTCTRoot.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	02 00 00 b9
Signature algorithm	sha1RSA
Issuer	Baltimore CyberTrust Root
	CN=Baltimore CyberTrust Root
	OU=CyberTrust
	O=Baltimore
	C=IE
Valid from	2000-05-12 18:46:00
Valid to	2025–05–12 23:59:00
Subject	Baltimore CyberTrust Root
	CN=Baltimore CyberTrust Root
	OU=CyberTrust
	O=Baltimore
	C=IE
Public key	RSA (2048 bits).
	Key bits are displayed in the lower pane of the window.
Key usage	Certificate Sign, CRL Sign
Subject key ID	e5 9d 59 30 82 47 58 cc ac fa 08 54 36 86 7b 3a b5 04 4d f0

Table 43. BTCTRoot.crt Certificate details (continued)

Certificate field	Default value/format
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	d4 de 20 d0 5e 66 fc 53 fe la 50 88 2c 78 db 28 52 ca e4 74

 $\textbf{Certificate name} - \texttt{Class3PCA\_G2\_v2.crt}$ 

Table 44. Class3PCA\_G2\_v2.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	7d d9 fe 07 cf a8 le b7 10 79 67 fb a7 89 34 c6
Signature algorithm	sha1RSA
Issuer	VeriSign Trust Network
	OU=VeriSign Trust Network
	OU=(c) 1998 VeriSign, Inc. – For authorized use only
	OU=Class 3 Public Primary Certification Authority – G2
	O=VeriSign, Inc
	C=US
Valid from	1998-05-18 00:00:00
Valid to	2028-08-12 23:59:59
Subject	VeriSign Trust Network
	OU=VeriSign Trust Network
	OU=(c) 1998 VeriSign, Inc. – For authorized use only
	OU=Class 3 Public Primary Certification Authority – G2
	O=VeriSign, Inc
	C=US
Public key	RSA (1024 bits).
	Key bits are displayed in the lower pane of the window.
Thumbprint algorithm	sha1
Thumbprint	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

 $\textbf{Certificate name} - \texttt{Class4PCA\_G2\_v2.crt}$ 

Table 45. Class4PCA\_G2\_v2.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	32 88 8e 9a d2 f5 eb 13 47 f8 7f c4 20 37 25 f8
Signature algorithm	sha1RSA
Issuer	VeriSign Trust Network
	OU=VeriSign Trust Network
	OU=(c) 1998 VeriSign, Inc. – For authorized use only
	OU=Class 4 Public Primary Certification Authority – G2

Table 45. Class4PCA\_G2\_v2.crt Certificate details (continued)

Certificate field	Default value/format
	O=VeriSign, Inc
	C=US
Valid from	1998-05-18 00:00:00
Valid to	2028-05-01 23:59:59
Subject	VeriSign Trust Network
	OU=VeriSign Trust Network
	OU=(c) 1998 VeriSign, Inc. – For authorized use only
	OU=Class 4 Public Primary Certification Authority – G2
	O=VeriSign, Inc
	C=US
Public key	RSA (1024 bits).
	Key bits are displayed in the lower pane of the window.
Thumbprint algorithm	sha1
Thumbprint	0b 77 be bb cb 7a a2 47 05 de cc 0f bd 6a 02 fc 7a bd 9b 52

 $\textbf{Certificate name} - \texttt{Entrust\_G2.crt}$ 

Table 46. Entrust\_G2.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	4a 53 8c 28
Signature algorithm	sha256RSA
Issuer	Entrust Root Certification Authority
	CN=Entrust Root Certification Authority—G2
	OU=(c) 2009 Entrust, Inc. – For authorized use only
	OU=See www.entrust.net/legal-terms.
	O=Entrust, Inc.
	C=US
Valid from	2009–07–07 17:25:54
Valid to	2030–12–07 17:55:54
Subject	Entrust Root Certification Authority
	CN=Entrust Root Certification Authority—G2
	OU=(c) 2009 Entrust, Inc. – For authorized use only
	OU=See www.entrust.net/legal-terms.
	O=Entrust, Inc.
	C=US
Public key	RSA (2048 bits).
	Key bits are displayed in the lower pane of the window.
Key usage	Certificate Sign, CRL Sign

Table 46. Entrust\_G2.crt Certificate details (continued)

Certificate field	Default value/format
Subject key ID	6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

Certificate name - EquafaxCA1.crt

Table 47. EquafaxCA1.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	04
Signature algorithm	md5RSA
Issuer	Equifax Secure eBusiness
	CN=Equifax Secure eBusiness CA-1
	0=Equifax Secure Inc.
	C=US
Valid from	1999-06-21 04:00:00
Valid to	2020-06-21 04:00:00
Subject	Equifax Secure eBusiness
	CN=Equifax Secure eBusiness CA-1
	0=Equifax Secure Inc.
	C=US
Public key	RSA (1024 bits).
	Key bits are displayed in the lower pane of the window.
Key usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign, Encipher Only, Decipher Only
Subject key ID	4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
Authority key ID	80 14 4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	da 40 18 8b 91 89 a3 ed ee ae da 97 fe 2f 9d f5 b7 d1 8a 41

Certificate name - gd-class2-root.crt

Table 48. gd-class2-root.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	00
Signature algorithm	sha1RSA
Issuer	Go Daddy Class 2 Certification Authority

Table 48. gd-class2-root.crt Certificate details (continued)

Certificate field	Default value/format
	OU=Go Daddy Class 2 Certification Authority
	O=The Go Daddy Group, Inc.
	C=US
Valid from	2004-06-29 17:06:20
Valid to	2034-06-29 17:06:20
Subject	Go Daddy Class 2 Certification Authority
	OU=Go Daddy Class 2 Certification Authority
	O=The Go Daddy Group, Inc.
	C=US
Public key	RSA (2048 bits).
	Key bits are displayed in the lower pane of the window.
Key usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign, Encipher Only, Decipher Only
Subject key ID	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3
Authority Key ID	Key bits are displayed in the lower pane of the window.
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	27 96 ba e6 3f 18 01 e2 77 26 1b a0 d7 77 70 02 8f 20 ee e4

Certificate name - GTECTGlobalRoot.crt

Table 49. GTECTGlobalRoot.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	01 a5
Signature algorithm	md5RSA
Issuer	GTE CyberTrust Global Root
	CN=GTE CyberTrust Global Root
	OU=GTE CyberTrust Solutions, Inc.
	O=GTE Corporation
	C=US
Valid from	1998-08-13 00:29:00
Valid to	2018-08-13 23:59:00
Subject	GTE CyberTrust Global Root
	CN=GTE CyberTrust Global Root
	OU=GTE CyberTrust Solutions, Inc.
	O=GTE Corporation
	C=US

Table 49. GTECTGlobalRoot.crt Certificate details (continued)

Certificate field	Default value/format
Thumbprint algorithm	sha1
Thumbprint	97 81 79 50 d8 1c 96 70 cc 34 d8 09 cf 79 44 31 36 7e f4 74

Certificate name—Pc32ss\_v4.crt

#### Table 50. Pc32ss\_v4.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	70 ba e4 1d 10 d9 29 34 b6 38 ca 7b 03 cc ba bf
Signature algorithm	md2RSA
Issuer	Class 3 Public Primary Certification Authority
	OU=Class 3 Public Primary Certification Authority
	O=VeriSign, Inc.
	C=US
Valid from	1996-01-29 00:00:00
Valid to	2028-08-01 23:59:59
Subject	Class 3 Public Primary Certification Authority
	OU=Class 3 Public Primary Certification Authority
	O=VeriSign, Inc.
	C=US
Public key	RSA (1024 bits).
	Key bits are displayed in the lower pane of the window.
Thumbprint algorithm	sha1
Thumbprint	74 2c 31 92 e6 07 e4 24 eb 45 49 54 2b e1 bb c5 3e 61 74 e2

Certificate name - PCA-3G5.crt

#### Table 51. PCA-3G5.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary Certification Authority — G5
	CN=VeriSign Class 3 Public Primary Certification Authority — G5
	OU=(c) 2006 VeriSign, Inc. – For authorized use only
	OU=VeriSign Trust Network
	O=VeriSign, Inc
	C=US
Valid from	2006-11-08 00:00:00
Valid to	2036-07-16 23:59:00

Table 51. PCA-3G5.crt Certificate details (continued)

Certificate field	Default value/format		
Subject	VeriSign Class 3 Public Primary Certification Authority — G5		
	CN=VeriSign Class 3 Public Primary Certification Authority — G5		
	OU=(c) 2006 VeriSign, Inc. – For authorized use only		
	OU=VeriSign Trust Network		
	O=VeriSign, Inc		
	C=US		
Public key	RSA (2048 bits).		
	Key bits are displayed in the lower pane of the window.		
Key usage	Certificate Sign, CRL Sign		
Subject key ID	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33		
Basic constraints	Subject Type=CA, Path Length Constraints=None		
Thumbprint algorithm	sha1		
Thumbprint	4e b6 d5 78 49 9b 1c cf 5f 58 le ad 56 be 3d 9b 67 44 a5 e5		

## Using the troubleshooting options

Use the **Troubleshooting** dialog box to configure trace and event log settings, performance monitor graphs that display client CPU, memory, and networking information, and CMOS management extract and restore CMOS settings. It also enables you to view the wnos.ini cached information for troubleshooting purposes.

To use the troubleshooting options:

- 1. From the desktop menu, click **Troubleshooting**. The **Troubleshooting** dialog box is displayed.
- 2. Click the **General** tab, and do the following:

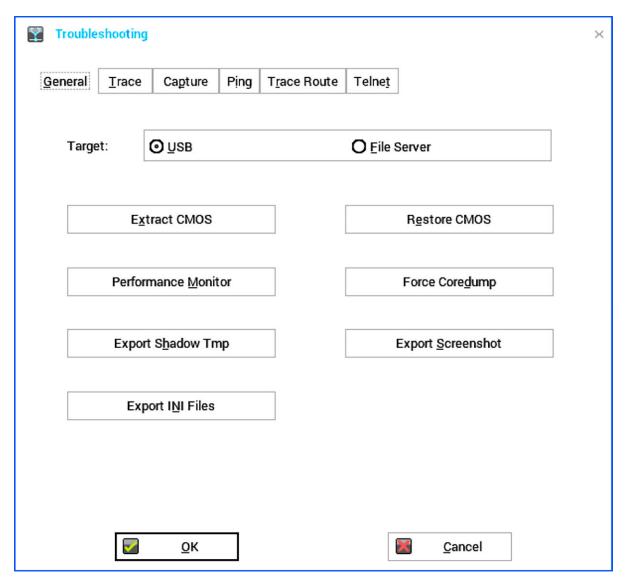


Figure 39. General

- · Click either **USB** or **File Server** to select your target device you want to use for CMOS management.
- **Extract CMOS**—Click this option to extract the CMOS settings and certain BIOS settings to the USB drive or file server based on your target device selection. ThinOS reads the CMOS settings from the SMBIOS Interface for Dell BIOS, and the CMOS interface for legacy Wyse BIOS. For information about the support matrix, see the *Dell Wyse ThinOS Version 8.6 Release Notes* at www.dell.com/support.
  - NOTE: You can only extract the BIOS settings that are supported by the INI parameter Device=CMOS and Device=DellCMOS.
- **Restore CMOS**—Click this option to write the CMOS settings and BIOS settings from the USB drive to the target thin client. For information about the support matrix, see the *Dell Wyse ThinOS Version 8.6 Release Notes* at www.dell.com/support.
  - NOTE: You can restore the BIOS settings that are supported by the INI parameter Device=CMOS and Device=DellCMOS.
- **Performance Monitor**—Click this option to display the CPU usage history with frames per second (FPS), Memory, and Networking information. The graphs display on top of all windows.
- Force Coredump—Use this option to forcibly generate the debug information for technical investigation when your system is not responding. Both the coredump file and the trap information image are saved to the local drive. After you restart the thin client, both the coredump file and trap issue screenshot file are uploaded to the /wnos/troubleshoot/ directory of the file server or a USB drive.
- **Export Shadow Tmp**—Use this option to export temporary logs for debugging purpose. All log files can be exported to a USB drive or file server depending on the target configuration.

- **Export Screenshot**—Use this option to export screenshots to the file server or a USB drive. The exported file name is added with build information for a better troubleshooting. If a screenshot is present in the clipboard, it is exported to the target location. If the screenshot is not available, the full screen is copied automatically and exported to the target location.
- **Export INI files**—Use this option to export the global INI file (wnos.ini or xen.ini), wdm.ini, ccm.ini, mac.ini, or other machine based INI file to the file server or a USB drive. Only username.ini file cannot be exported.
- 3. Click the **Trace** tab to configure the trace actions and delay on trace. The available options for trace action are None, Capture, and Playback.



Figure 40. Trace

4. Click the **Capture** tab, and configure the export event log, network capture, wireless capture, and capture USB packets as per your requirements.

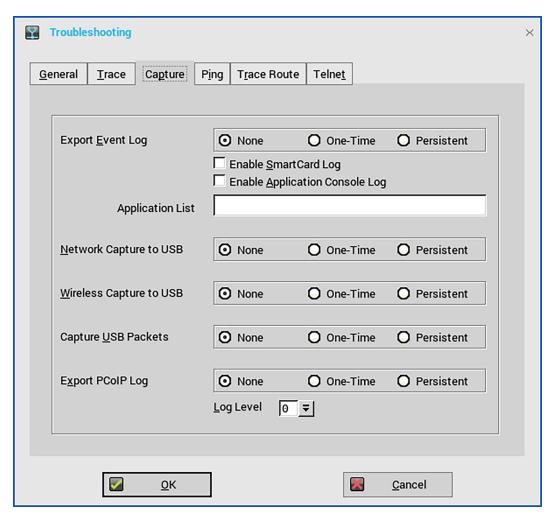


Figure 41. Capture

- a. **Export Event log**—Click either the **One-time** or **Persistent** option to enable logging any unexpected error messages. You can turn off logging and check the log file under the folder https:/wnos/trouble\_shoot. Ensure to enable the **Enable Trace** option of the Privilege parameter in a wnos.ini file. For more information, see the *Dell Wyse ThinOS INI Guide*.
- Enable SmartCard log—To enable the client to log error messages of the smart card, select the Enable SmartCard log check box.
- c. Enable Application Console Log—To enable the client to log error messages of an application console, select the Enable Application Console Log check box. All logs are saved to the trouble\_shoot folder with the name TerminalName\_proc\_name\_date\_time.log.
  - In the **Application List** field, enter the name of the application for which you want to generate logs. The name in the list can be part of the application name. For example, the PCoIP application name is /pcoip/pcoip and blast application name is /usr/lib/vmware/view/usb/horizon. If you want to generate logs for both PCoIP and Blast applications, enter **pcoip; vmware** in the **Application List** field. By default, the **Application List** filters are not applied and all logs are saved to the target folder.
- d. **Network capture to USB**—Click either the **One-time** or **Persistent** option to enable the capture of network information. Enabling this option captures the network trace of all traffic coming in and out of the thin client to a USB drive that is inserted into the thin client.

After you log in and use the Citrix Apps and Desktops server or network, you can view the  $/wnos/troubleshoot/[Terminal Name]_[ENET or WS].[Date_Time].pcap file in the USB drive. You can analyze using software such as a packet analyzer used for network troubleshooting, and analysis.$ 

For example, for Ethernet, the file name is yx008064b2bfd7\_ENET.20150415\_064455.pcap. For wireless, the file name is yx008064b2bfd7\_WS.20150415\_064455.pcap.

NOTE: Ensure that you have inserted the USB drive into the thin client before selecting the network capture option. If the USB drive is not inserted and you exit the dialog box, the network capture is automatically cleared.

- e. Wireless capture to USB—Click either the One-time or Persistent option to enable the capture of wireless network information. Enabling this option captures the wireless network trace of all traffic coming in and out of the thin client to a USB drive that is inserted into the thin client.
- f. Capture USB Packets—Click either the One-time or Persistent option to enable the capture of USB packets.
- g. Export PCoIP log—Click either the One-time or Persistent option to export PCoIP logs on the PCoIP-enabled clients.
- 5. Click the Ping tab, and use the following guidelines to start the ping-diagnostic utility and display response messages:

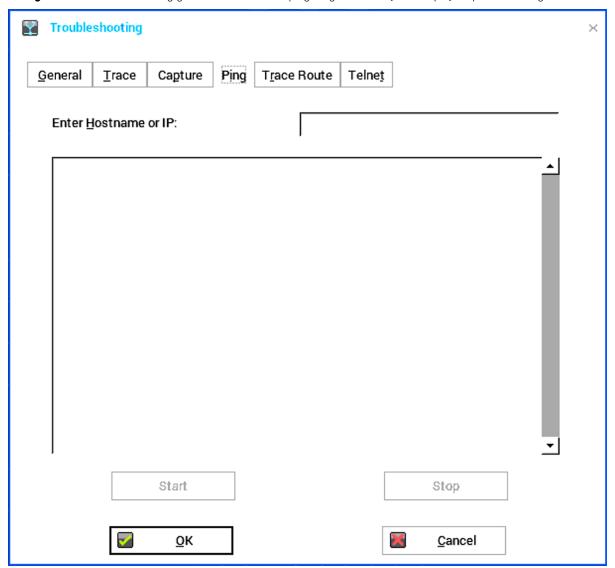


Figure 42. Ping

- Enter Hostname or IP—Enter the IP address, DNS-registered hostname, or WINS-registered hostname of the target to be pinged.
- **Data area**—Displays ping response messages. The ping command sends one echo request per second, calculates round trip times and packet loss statistics, and displays a brief summary upon completing the calculation.
- **Start**—Executes the ping command. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted by clicking **Stop**.
- · Stop—Terminates the ping request and leaves the Ping dialog box open, so you can read the summary posted in the data area.

#### (i) NOTE:

Ping sends an echo request to a network host. The host parameter is either a valid hostname or an IP address. If the host is operational and on the network, it responds to the echo request. Ping sends one echo request per second and calculates round trip times and packet loss statistics. It displays a brief summary upon completion of the calculation.

The ping utility can be used to:

- Determine the status of the network and various foreign hosts.
- Track and isolate hardware and software problems.
- · Test, measure, and manage networks.
- Determine the IP address of a host if only the hostname is known.
- NOTE: Not all network equipment responds to ping packets, as this is a common mechanism that is used in denialof-service attacks. Lack of response does not necessarily indicate that the target of the ping is unusable for other purposes.
- 6. Click the Trace Route tab, and use the following guidelines to start the tracert diagnostic utility and display response messages.

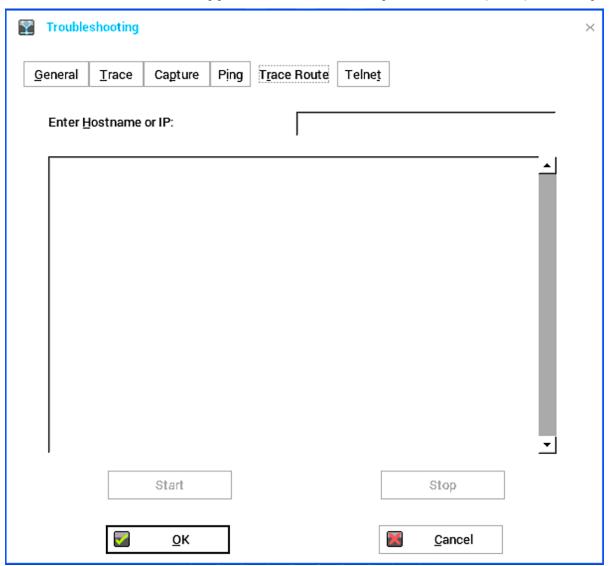


Figure 43. Trace route

- Enter Hostname or IP—Enter the IP address, DNS-registered hostname, or WINS-registered hostname of the target to be traced.
- Data area—Displays round-trip response time and identifying information for each device in the path.
- · Start—Executes the tracert command.
- Stop—Terminates the tracert command and leaves the Trace Route dialog box open, so that you can read the information
  posted in the data area.

The tracert utility traces the path from your thin client to a network host. The host parameter is either a valid hostname or an IP address. The tracert utility sends out a packet of information three times to each device (routers and computers) in the path and displays the round trip response times and identifying information in the message box.

7. Click the **Telnet** tab, and do the following:

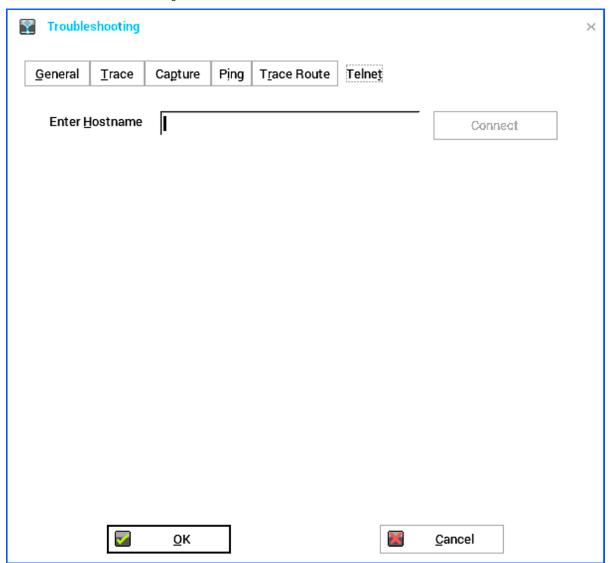


Figure 44. Telnet

- a. Enter the hostname.
- b. Click Connect to connect to a remote host or device.
   The Telnet window is displayed, and the troubleshooting window is closed automatically.

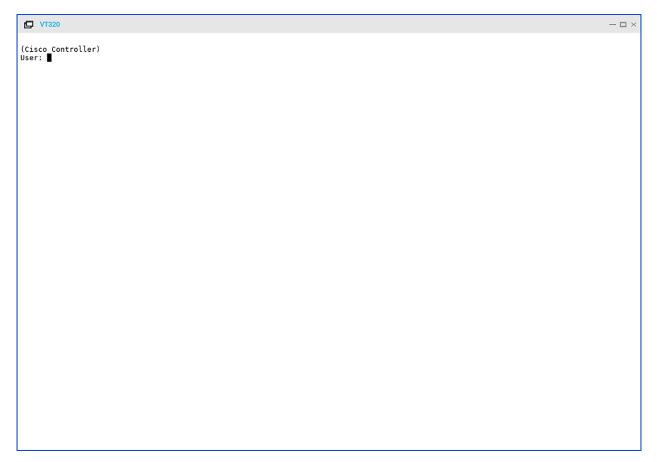


Figure 45. Telnet window

8. Click  $\mathbf{OK}$  to save your settings.

## **BIOS management on ThinOS**

This appendix describes the BIOS management on the ThinOS devices with Wyse BIOS (CMOS), or Dell Standard BIOS.

To make the BIOS management consistent between Wyse BIOS and Dell BIOS, an INI parameter Device=Cmos is introduced for Wyse BIOS, and Device=DellCmos for Dell Standard BIOS.

If the password is configured for the BIOS configuration, then you must enter an appropriate password to update any settings. For example, the INI parameter to update settings must be followed with "CurrentPassword={}". This is mandatory for Dell BIOS.

After you update BIOS on Wyse 5010 thin client, Wyse 5040 thin client, Wyse 7010 thin client, Wyse 5060 thin client, and Wyse 3030 LT thin client by using file server, the BIOS management may not be possible until you manually enter and exit the BIOS configuration menu. This is due to a CMOS mismatch. To resolve this issue:

- · Boot unit and press Delete during boot to enter the BIOS menu.
- · Enter the BIOS password.
- · Press F10 to save BIOS configurations and resolve the CMOS mismatch.

#### **BIOS functionality matrix**

#### Table 52. BIOS functionality matrix

Major requirement	INI parameter 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
Power on without beeps	N/A	Yes	Yes	Yes	Yes
Update BIOS from file server	N/A	Yes	Yes	Yes	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	Yes	Yes	Yes	Yes

Table 52. BIOS functionality matrix (continued)

Major requirement	INI parameter 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
	AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Fri day				
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

## **Accessing BIOS settings**

After starting your thin client, you will see a Dell logo for a short time. During this period, press and hold the Delete key or F2 key based on the thin client model.

- · Delete key—Press and hold the Delete key to enter the BIOS settings on the ThinOS clients with Wyse BIOS.
- · F2 key—Press and hold the F2 key to enter the BIOS settings on the ThinOS clients with Dell Standard BIOS.

When prompted, type the password **Fireport** to view the BIOS settings screen. For example, you can use the F7 key to use Optimized Defaults—load optimal default values for all the items in the BIOS setup utility.

NOTE: These BIOS settings are not applicable to Wyse 3010 thin client and Wyse 3020 thin client, as there is no BIOS on ARM platform. To accessWLOADER on an ARM platform, press the power button for four seconds until the power light turns green, and then press the Delete key.

# CMOS central management and extracting CMOS settings to the file server for distribution

CMOS central management allows ThinOS administrators to easily manage CMOS settings for large deployments of thin client devices using central configuration methodologies. Wyse 5010 thin client with ThinOS (D10D) is considered here as an example. The following instructions are for Wyse 5010 thin client with ThinOS (D10D) BIOS version 3.0D. However, the instructions are also applicable for other supported hardware platforms and BIOS versions.

- 1. To prepare a reference drive containing BIOS version 3.0D or later:
  - a. The reference device is a golden image you use to distribute to other thin client devices. To use reference drive, enter the BIOS setup utility. Press the **Delete** key, enter the password **Fireport** (case sensitive) and press **Enter**. Configure the CMOS settings, includes Auto Power, Boot Order, P-key setting, and BIOS Password.
  - b. Save your CMOS settings.
  - c. Restart your thin client device.
- 2. To create a CMOS INI file in a file server:
  - a. In the file server, create a cmos.ini file and place it in the wnos directory/folder under the file server ini directory. Make sure that wnos directory on the file server has upload privilege.
  - b. Type the following name in the cmos.ini file: **Device=cmos Action=extract**.
- 3. To reboot the reference device to the file server containing the CMOS INI file:
  - a. On the thin client you want to use as a reference device, start the thin client.
  - b. In the Login dialog box, enter the credentials you need to access the cmos.ini file.
  - c. After login, to view the **Event Log** tab, do the following:

#### Click System Information icon > System Information dialog box > Event Log tab.

You can open the event log to view a CMOS: extract to D10D\_cmos.3.0D event. This means that the CMOS central management file (containing the CMOS settings from your Reference Device) is now copied to the wnos directory/folder on the file server. As this is a D10D BIOS version 3.0D, the CMOS central management file name would be D10D\_cmos.3.0D. These CMOS settings are now ready for distribution to other thin clients.

- **4.** To prepare the file server containing the CMOS INI file for distribution:
  - a. Write the following line in the cmos.ini file for distribution on your file server: **Device=cmos Action=restore**.
  - b. Save the file.
- 5. Log in to all target device to the file server containing the CMOS INI file:
  - a. Start the thin client devices for which you want to distribute the reference device CMOS settings.
  - b. To access the cmos.ini. file, enter your credentials in the Login dialog box.
  - c. To open Event Log, click System Information icon. In the System Information dialog box, select Event Log tab. You can view the CMOS: restore from D10D\_cmos.3.0D event. This means that your central management file containing the CMOS settings from your reference device is copied to the targeted thin client devices.
  - NOTE: After you target your thin client devices contain the CMOS settings you want, do not log in to the file server containing the cmos.ini file with the restore action (unless you want to redo the restore process). Administrators can remove the cmos.ini file to prevent from unwanted CMOS overwrites.
  - NOTE: It is recommended to initially complete these procedures on a file server designated to test the success of your CMOS central management settings/process. While the central configuration method can be used to enforce your CMOS settings in a production environment, be aware that any thin client device that logs in to the file server that contains the cmos.ini and its extract and restore commands are subject to those commands (CMOS overwrites).

For more information about the INI parameter Device=cmos, see Dell Wyse ThinOS INI Reference Guide.

# CMOS local management and extracting CMOS settings to a USB key for distribution

CMOS local management allows ThinOS administrators to easily manage CMOS settings for small deployments of thin clients using USB key distribution methods. Wyse 5010 thin client with ThinOS (D10D) is considered here as an example. The following instructions are for Wyse 5010 thin client with ThinOS (D10D) BIOS version 3.0D.

- 1. To prepare a reference drive containing BIOS version 3.0D or later:
  - a. The reference device is a golden image you use to distribute to other thin client devices. To use reference drive, enter the BIOS setup utility. Press the **Delete** key, enter the password **Fireport** (case sensitive) and press **Enter**. Configure the CMOS settings, includes Auto Power, Boot Order, P-key setting, and BIOS Password.
  - b. Save your CMOS settings.
  - c. Restart your thin client device.
- 2. To extract the CMOS settings to a USB key.

- a. Attach a formatted USB key on the thin client device which you want to use as a reference device. For example, to format on Windows 7, attach the USB Key, right-click the USB key, select format, click Restore device defaults, select Quick Format, and then click Start.
- b. Use the extract CMOS to USB GUI feature of ThinOS to extract the CMOS settings to the USB key. On Classic Desktop, right-click the desktop and select Extract CMOS to USB. On Wyse Zero desktop, in the General tab of the System Tools dialog box (System Settings icon > System Tools > General tab), click Extract CMOS to USB.
- **c.** Once extraction successful you see a pop-up message: CMOS: extract to D10D\_cmos.3.0D, properly eject and detach the USB key. The CMOS settings on the USB key are now ready for distribution to other thin clients
- **3.** To restore the CMOS settings to your target devices:
  - a. On all of the target thin clients that you want to distribute the reference device CMOS settings, start the thin client.
  - b. Use the Restore CMOS from USB GUI feature of ThinOS to write the CMOS settings from the USB Key to the target thin client: For Classic Desktop, Right-click the desktop and select Restore CMOS from USB. For Wyse Zero Desktop, in the General tab of the System Tools dialog box ( System Settings icon > System Tools > General tab), click Restore CMOS from USB.
  - c. Once restoration successful the following message is displayed: CMOS: restore from D10D\_cmos.3.0D properly eject and detach the USB Key. The CMOS settings on the USB Key are now written to your target thin client.

## **Dell Standard BIOS management**

This section describes how to configure and manage the ThinOS clients with Dell Standard BIOS.

#### Supported devices

- Wyse 3040 thin client with ThinOS
- · Wyse 3040 thin client with PCoIP
- · Wyse 5070 thin client with ThinOS
- Wyse 5070 Extended thin client

The following Dell BIOS configurations are supported by using file server (INI parameters):

#### Table 53. BIOS configuration options

Parameters	Settings	
System Configuration	Audio	
Security	<ul> <li>Admin Setup Lockout</li> <li>Admin Password</li> <li>Enable/Disable Admin Password</li> <li>Update Admin Password</li> </ul>	
USB Configuration	<ul><li>Enable Front USB Ports</li><li>Enable Rear-Left Dual USB 2.0 Ports</li></ul>	
Power Management	<ul> <li>Wake-On-LAN</li> <li>Disabled</li> <li>LAN Only</li> <li>LAN with PXE Boot</li> <li>AC Recovery</li> <li>Power Off</li> <li>Power On</li> <li>Last Power State</li> <li>Auto-On Time</li> <li>Disabled</li> <li>Every Day</li> <li>Weekdays</li> <li>Select Days</li> <li>Wake-On-USB</li> </ul>	
Device boot	USB boot     PXE boot	

For information about INI parameters and their usage, see the latest Dell Wyse ThinOS INI Reference Guide.

The following are examples of INI parameters:

- $\cdot \quad \text{Device=DellCmos newpassword=1234567 or newpasswordenc=encrypted strings} \\ \text{Use this INI parameter to create the admin password when password is not set}.$
- Device=DellCmos currentpassword=1234567 newpassword="" or currentpasswordenc=encrypted strings —Use this INI parameter to clear the existing password.

# **Security**

A new global security policy has been defined for ThinOS and this policy is applied to all secure connections (https/SSL connections) with a few exceptions.

**Purpose**—To improve the security level by default and add the global configuration. This security policy integrates security setting for each application.

#### Table 54. INI parameter

INI parameter	Description
SecurityPolicy={full   <b>warning</b> (default)   low}	<b>Full</b> —SSL connection must verify the server certificate. If it is untrusted, cancel the connection.
SecuredNetworkProtocol={yes   no (default)} TLSMinVersion={1 (default), 2, 3} TLSMaxVesion={1, 2, 3 (default)}	<b>Warning (default)</b> —SSL connection must verify the server certificate. If it is untrusted, you can continue or cancel the connection.
	<b>Low</b> —Server certificate is not verified. This value is set for a few applications.
	After firmware is updated, the default value is set to warning for all applicable applications immediately.
	There is an exception for file server and WDM.
	The old ini SecurityLevel   SecureProtocol from Privilege segment is deleted.

All applications running on the default SSL security mode follow the global mode. In the global mode, the default value is Warning. The affected applications include VMware View, Amazon WorkSpaces (AWS), file server, WDM Service, Caradigm Server, and OneSign Server.

For more information about the security mode INI parameters, see Dell Wyse ThinOS INI Guide.

The following are the exceptions:

- File server and WDM in factory reset state—Before you load any INI parameter, the SSL security mode is set to Low, and after loading the INI parameter, the value is changed to follow the global mode value. For example, the default value is set to warning, if the value is not changed by the INI parameter.
  - System with previous settings (default value is set to Low) follows the global mode after the unit is upgraded. For example, the default value is set to Warning, if the value is not changed by the INI parameter.
- VMware View and AWS brokers include own security settings (GUI and INI). From ThinOS 8.3 release, an additional option is added to
  follow the global mode as its new default value. The security mode GUI context is updated for better understanding.
- · Wyse Management Suite, Microsoft RDS broker, Citrix broker, and SecureMatrix are always Full.

## Firmware signature

Firmware signature feature was introduced in ThinOS 8.3.1 for better firmware security. From ThinOS 8.4 release, firmware signature verification is added to enhance firmware security.

#### Salient features

- By default, signature verification is required on firmware downgrade/upgrade process.
- Provision to downgrade from 8.4 firmware to 8.3 firmware without signature. For example, earlier to ThinOS 8.3.1 release, the firmware downgrade is prohibited by default.
- New INI parameter verifysignature=no is introduced to enable user downgrade firmware. For example: autoload=101 verifysignature=no. For more information about using INI parameters, refer to the latest Dell Wyse ThinOS INI Reference guide.

The following scenarios are allowed without need of using INI parameters:

• Upgrade from 8.3.x firmware to 8.4 firmware.

- o Upgrade or Downgrade between 8.3.x and/or earlier firmware.
- Upgrade or Downgrade between 8.4 and later firmware.

## **Transport Layer Security**

Transport Layer Security (TLS) is a protocol that provides communication security between the client and server applications.

**Upgrade to Transport Layer Security (TLS)**— In the ThinOS 8.2 release, the TLS is upgraded from version 1.0 to version 1.2. By default, the ThinOS client uses TLS 1.2 to secure any communication protocols, connections, or applications upon SSL/ TLS in general and falls back to the previous SSL/ TLS version when negotiating with the server.

## Smart cards and smart card readers

A smart card is a security token that has embedded integrated circuits. Smart cards allow you to store and transact data.

A smart card reader is an input device that reads data from a smart card.

• **Gemalto smart card IDPrime MD840**—Gemalto smart card IDPrime MD830 and MD840 are supported. IDGo 800 version 1.2.1 - 01 for the Windows middleware is required for supporting Gemalto smart card IDPrime MD840.

The Secure Messaging feature is supported to enable the usage of latest MD830 Rev B cards.

Known issue for Prime MD 840 smart card: If first container is used, then Xen broker logon fails.

- **OMNIKEY smart card readers**—The following OMNIKEY smart card readers are supported:
  - o Omnikey 5427 CK (0x5427, 0x076b) reader supports iclass15693, 14443a, 125k card
  - o Omnikey 5422
  - o Omnikey 5326 DFR (0x5326, 0x076b) reader supports iclass15693 card
  - o Omnikey 5025 CL (0x502a, 0x076b) reader supports 125k card
  - o Ominkey 5325 CL, 5125 (0x5125, 0x076b) reader supports 125k card
  - Omnikey 5321 V2 CLi (0x532a, 0x076b) reader supports 13.56 MHz card
  - Omnikey 5321 V2 (076b, 5321) reader supports 13.56 MHZ card
  - o Omnikey 5021 CL (0x5340, 0x076b) reader supports 13.56 MHZ card
  - o Omnikey 5321 V2 CI Sam (0x5341, 0x076b) reader supports 13.56 MHz card
  - Omnikey 5421 (0x5421, 0x076b), reader supports 13.56 MHz card
  - Omnikey 5321 CR (0x5320, 0x076b)
  - o Omnikev 5022 CL
- On-board smart card reader—On-board smart card reader works with regular smart cards. The functionality is similar to other
  external USB smart card readers and on-board smart card readers such as Dell KB-813.
- · TicTok smart cards—ThinOS supports TicTok smart cards.
- ThinOS supports Cryptovision smart card driver cv\_act\_scinterface\_7.1.5 from this release.

For information about the complete list of the tested smart cards and smart card readers, see the latest Release Notes.

### Rutoken smart card reader

Rutoken is a USB smart card that is used for two-factor authentication. You can generate and store encryption keys for electronic signatures, use it to encrypt keys, and perform electronic signature. You can also use this device to encrypt store digital certificates and other data.

ThinOS 8.6 MR3 supports Rutoken 2151 and Rutoken ECP 2.0 (2100).

# **Troubleshooting**

This section describes some basic troubleshooting that you can implement when you experience any problem.

• ThinOS devices allow secure SSL connections—SecurityMode=Full—only after verifying the certificates. In the present scenario, the devices enforce the warning policy after you define a server using a valid IP address.

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.
- 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
- Blast connection—If there is a launch issue, check the remote desktop status and network status; reboot unit few times and the desktop connects successfully.

## **Examples of common printing configurations**

This appendix provides examples on using the **Printer Setup** dialog box and ThinOS INI parameters for common printing situations. Use these general guidelines in addition to the information provided in Configuring the Printer Setup.

(i) NOTE: Host-based printers are not supported.

#### It includes:

- · Printing to local USB or parallel printers
  - Using the Printer Setup dialog box for local USB or parallel printers
  - o Using INI parameters for local USB or parallel printers
- · Printing to non-Windows network printers (LPD)
  - Using the Printer Setup dialog box for non-Windows network printers (LPD)
  - o Using INI parameters for non-Windows network printers
- Printing to Windows network printers (SMB)
  - o Using the Printer Setup dialog box for Windows network printers
  - Using INI parameters for Windows network printers
- Using your thin client as a print server (LPD)
  - Using the Printer Setup dialog box for configuring LPD services
  - o Using INI parameters for configuring LPD services
- · Configuring ThinPrint

## Printing to local USB or parallel printers

You can print to locally attached printers through USB or parallel ports.

NOTE: Microsoft Remote Desktop Session Host (RDSH), Microsoft Terminal Services, and Citrix XenApp each have their own printing policies that must be configured properly to allow client side printing. For details on configuring printing in these environments, see your vendor instructions.

# Using the Printer Setup dialog box for local USB or parallel printers

In this example you have an HP LaserJet 4000 attached to a thin client USB port. When connecting USB printers, some printers fill out the Printer Name and Printer Identification fields for you.

To Configure the Printer to print locally attached printers through USB or Parallel ports.

- From the desktop menu, click System Setup > Printer.
   The Printer Setup dialog box is displayed.
- 2. Click Printer Setup, and use the following guidelines for the Ports tab when printing to a local USB printer:
  - a. Select Port Select LPT1 or LPT2 port.
  - b. **Printer Name** Enter name you want displayed in your list of printers, most USB direct-connected printers report/fill in their printer name automatically.
  - c. Printer Identification Enter the type or model of the printer in the exact text of the Windows printer driver name including capitalizations and spaces most USB direct-connected printers report/fill in their printer identifications automatically. In our example case, enter HP LaserJet 4000 Series PCL.
  - d. Printer Class You can leave this as default.
  - e. Enable the printer device Must be selected to enable the directly connected printer enables the device so it displays on the remote host.
- 3. Click **OK** to save the settings.

### Using INI parameters for local USB or parallel printers

Configuring local printing using ThinOS INI parameters is simple and an easy way to configure a printer for all clients in your environment assuming every printer is the same.

Your INI parameters will look something like the following:

```
Printer=LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled=yes
```

NOTE: The PrinterID is the exact text of the Windows printer driver name, so if a printer driver is named HP LaserJet 4000 Series PCL in Windows, then it must be exactly the same in the PrinterID field in the INI parameters including capitalizations and spaces.

## Printing to non-Windows network printers

ThinOS can print to non-Windows network printers as long as the printers can accept LPR print requests. Most workgroup printers and large network printers have this capability be sure to check with your vendor that the printer can accept Line Printer Request print requests.

Once your thin client is configured to print to an LPR capable printer, the client will then redirect this printer through an RDP or ICA connection to your back end infrastructure. In this way the client will connect to your back end infrastructure and this network printer will appear as a client local printer.

# Using the Printer Setup dialog box for non-Windows network printers

To configure the **Printer Setup** dialog box for Non-Windows Network Printers (LPD).

- 1. From the desktop menu, click **System Setup**, and then click **Printer**.
  - The **Printer Setup** dialog box is displayed.
  - In this example we have an HP LaserJet 4200n attached to a thin client through LPR.
- 2. Click the LPDs tab and use the following guidelines when printing to a non-Windows network printer:
  - a. Select LPD Select LPD1 or LPD2 port.
  - b. Printer Name Enter name you want displayed in your list of printers.
  - c. **Printer Identification** Enter the type or model of the printer in the exact text of the Windows printer driver name including capitalizations and spaces.
    - In this example, enter HP LaserJet 4200n PCL6.
  - d. LPD Hosts The DNS or WINS name of the server for the network printer. An IP address of the printer on the network can also be entered as we have used in our case example.
    - NOTE: If the printer is attached to another thin client on your network, the entry in the LPD Hosts box is the name or address of that thin client.
  - e. LPD Queue Name An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer used. This name can be different for each vendor. This field is required and must be correct so that the network printer accepts incoming print jobs properly. In our case example, auto can be used for HP LaserJet 4200n PCL6 as per documentation found on the HP website.
    - NOTE: If the printer is attached to another thin client on your network, the LPD Queue Name must match the content of the Printer Name box on the thin client with the printer attached.
  - f. Printer Class —You can leave this as default.
  - g. Enable the printer device Must be selected to enable the printer enables the device so it displays on the remote host.

## Using INI parameters for non-Windows network printers

Configuring network printing using ThinOS INI parameters is simple and an easy way to configure a printer for all clients in your environment assuming every printer is the same.

Your INI parameters will look something like the following:

```
Printer=LPD1 \
LocalName="HP LaserJet 4200n" \
Host=10.10.10.1 \
Queue=auto \
PrinterID="HP LaserJet 4200 PCL6" \
Enabled=yes
```

NOTE: The PrinterID is the exact text of the Windows printer driver name, so if a printer driver is named HP LaserJet 4200n PCL6 in Windows, then it must be exactly the same in the PrinterID field in the INI parameters including capitalizations and spaces.

## **Printing to Windows network printers**

ThinOS can print to printers that are shared by Microsoft print servers. There are some configuration requirements that need to be considered when configuring SMB printing from ThinOS which may require changes to your thin client setup.

Since connecting to a Microsoft Windows Print Server requires domain credentials, you must provide the credentials to ThinOS either on demand as the printer is used or by administrator setup providing credentials cached from the Dell Wyse login screen, see Example 3: **Defining an SMB Printer to Use User Credentials Cached by ThinOS (Advanced)** in Using INI parameters for Windows network printers (SMB). This section will discuss both methods.

# Using the Printer Setup dialog box for Windows network printers

Configuring an SMB printer is this manner forces users to enter their credentials before each printing; this means they will be temporarily pulled out of their remote session to enter their credentials (this can be avoided by using an INI file as discussed in Using INI parameters for Windows network printers.

- From the desktop menu, click System Setup > Printer.
   The Printer setup dialog box is displayed.
- 2. Click the SMBS tab, and use the following guidelines when printing to a Windows network printer:
  - i NOTE: The printer name shared by Windows must not contain any spaces or ThinOS will not be able to use it.
  - a. **Select SMB** Select the SMB you want from the list.
  - b. \\Host\Printer Click the browse folder icon next to the box to browse your Microsoft Networks and make the printer selection you want from the network printers available the DNS name or IP address of the Windows print server on the network. After entering required domain credentials, the **Printer Setup** dialog box will display
  - c. Printer Name Enter name you want displayed in your list of printers.
  - d. **Printer Identification** Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.
    - In example case, enter HP LaserJet 4100 Series PCL.
  - e. Printer Class You can leave this as default.
  - f. Enable the printer device Must be selected to enable the printer.

It enables the device so it displays on the remote host.

Click **Test Print** and you will be prompted to enter your Windows credentials, these credentials will be used to access the printer share. This is also the same dialog box that will display for a user when they attempt to print to this printer.

## Using INI parameters for Windows network printers

Configuring SMB printing using ThinOS INI parameters is simple and an easy way to configure printers shared by a Windows server for all clients in your environment. The primary advantage of configuring SMB printing using ThinOS INI parameters is that you can pre-define the domain account to use to authenticate the printer. The following examples discuss how the credentials can be supplied.

1. Defining an SMB printer with generic user credentials in plain text

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=Username1 \
Password=Password \
Domain=contoso
```

2. Defining an SMB printer with generic user credentials that are encrypted

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username-enc=PACGOGDBPKDOPGDGKC \
Password-enc=PFDBOHDBODCJPODP \
Domain=contoso
```

- NOTE: You can use the Configuration Generator (ConfGen) tool to create INI parameters for ThinOS. ConfGen can be downloaded from technicalhelp.de.. This is a non-supported tool that is linked solely for the purpose of this example.
- 3. Defining an SMB printer to use user credentials cached by ThinOS (advanced)
- NOTE: This method requires that the user log in to ThinOS so that the credentials can be cached for later use. The example INI section provided below provides the minimum requirements you need.

Signon=NTLM

```
Connect=RDP \
Host=1.2.3.4 \
Username=$UN \
Password=$PW \
Domain=$DN \
AutoConnect=1

Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=$UN \
Password=$PW \
Domain=$DN
```

## Using your thin client as a print server

ThinOS thin client can be configured as a basic network print server, to share local printers with other thin clients.

# Using the Printer Setup dialog box for configuring LPD services

From the Classic desktop mode only, a thin client can be configured to provide LPD (Line Printer Daemon) services making the thin client a printer server on the network. Set up the thin client that is to provide LPD print services as follows:

To configure LPD services using the Printer Setup dialog box.

- 1. From the desktop menu, click **System Setup > Network Setup** to open the **Network Setup** dialog box.
- 2. Enter a static IP address for the thin client.
- 3. From the desktop menu, click **System Setup** > **Printer** to open the **Printer Setup** dialog box and select any of the listed ports.
- 4. Select a LPT.
- 5. Name the printer in the **Printer Name** box.
- 6. Enter the **Printer Identification** type or model of the printer in the exact text of the Windows printer driver name including capitalizations and spaces. In our example case, enter HP LaserJet 4000 Series PCL.
- 7. You can leave **Printer Class** as default.
- 8. Select Enable the Printer Device.
- 9. Select Enable LPD service for the printer.
- 10. For setting up Windows 2003/2008 servers, see Setting up Windows 2003/2008 servers.

### **Setting up Windows servers**

To configure setting the Windows 2003/2008 servers

- Navigate to Control Panel > Administrative Tools > Services and ensure the Microsoft TCP/IP Printing service is installed. If it is not, install it using the Microsoft installation instructions.
- 2. Add the thin client as the LPD printer by completing the following:
  - a. Navigate to Control Panel > Printers > Add Printers > Local Printer > Create a new port and select LPR PORT.
    - i NOTE: If you do not see LPR Port, ensure that the Microsoft TCP/IP Printing service is installed correctly.
  - b. Type the thin client IP address or DNS name in the Name or address of host providing LPD box.
  - c. Type the printer name assigned in Using the Printer Setup dialog box for configuring LPD services in the Name of printer on that machine box.
  - d. Click OK, and then click NEXT.
- **3.** After you have selected the printer, you can perform your normal printer setup for the application server. For example, select the manufacturer printer type and printer name.

## Using INI parameters for configuring LPD services

Configuring LPD printing using ThinOS INI parameters is simple and an easy way to configure a ThinOS thin client to be a basic network print server, to share local printers with other thin clients.

Your INI parameters will look something like the following:

```
Printer=LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled=yes \
EnableLPD=yes
```

NOTE: The PrinterID is the exact text of the Windows printer driver name, so if a printer driver is named HP LaserJet 4000 Series PCL in Windows, then it must be exactly the same in the PrinterID field in the INI parameters including capitalizations and spaces.

## **Configuring ThinPrint**

No ThinPrint specific configuration is available on the thin clients. Thus to be able to use ThinPrint, users must first set up their printers according to the user documentation, and then configure ThinPrint on the thin client using the Printer Setup dialog box.

To configure the ThinPrint, use the following guidelines:

- · Use the **Printer Identification** field to enter a printer class (you can change the printer name as needed).
- · Printer IDs are assigned (depending on the physical port) as follows:
  - o COM1 = 1
  - o COM2 = 2
  - o LPT1 = 3 USB printers are detected automatically on LPT1
  - LPT2 = 4
  - o LPD0 = 5- The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - LPD1 = 6 The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - o LPD2 = 7 The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - o LPD3 = 8 The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - SMB1 = 9 In the form \\host\printershare
  - o SMB2 = 10
  - o SMB3 = 11
  - o SMB4 = 12

To install the relevant ThinPrint product on the server use the following guidelines:

- Printer Objects Created Manually by the Administrator After you install.print Engine, create a printer object on the server to use the native driver and ThinPort as a printer port. You can use any protocol (TCP, RDP or ICA) because ThinOS has.print clients for all of the protocols. The printer object needs to observe ThinPrint naming conventions, for example, HPLJ5#\_:2, in which case print jobs are sent to the local printer that has ID number .2 by referring to.print client port ID. If no ID number is present, the.print client sends the print job to the printer set as current.
- **Printer Objects Created Automatically by ThinPrint AutoConnect** When using ThinPrint AutoConnect, the thin client identifies with the thin client ID number 84 and thus is recognized as a thin client without a local spooler. You can also set up a template on the server that uses a native driver example, *HPLJ5*) and ThinPort, and then name this template as you want in the form \_#AnyName.

You can then make sure that the rules on ThinPrint Autoconnect [1] have been set to assign the desired local printers to use this server template. The assigned printer will then be shown in the user session using the HPLJ5 driver and ThinPort; it is named automatically according to ThinPrint naming convention with the printer name from the client side included. Alternatively, you can also define a template name according to the client printer name (replace.AnyName. with printer name 4. and 5. above for example, \_#HP Laserjet 5 so that the local printer object.HP Laserjet 5. is mapped to this template without any rules defined on the ThinPrint Autoconnect.

## Important notes

- VNC RFB version upgrade—Since ThinOS 8.0\_214, the VNC RFB version has been upgraded to 3.8. This version upgrade provides support for applications like DameWare. Thus, an administrator can now remote into a ThinOS device using either DameWare or VNC Viewer. Prior to 8.0\_214, you could only use VNC Viewer.
- **Headless boot**—ThinOS supports the headless mode that enables you to boot the operating system without a monitor.
- Report locally attached devices to Wyse Device Manager From ThinOS version 8.6, the locally attached devices such as monitor and USB device are reported to the Wyse Device Manager (WDM) server. This information is displayed in the device detail section on the WDM console.
  - NOTE: ThinOS supports more than 20 USB devices through the USB hub. However, WDM server shows only 10 devices.

# Frequently asked questions

This section contains information about the frequently asked questions (FAQs).

# How to enable USB Redirection in RDP windows 10 session

To enable USB Redirection in RDP windows 10 session, you must change the policy. Go to Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Service > Remote Desktop Session Host > Device and Resource Redirection > Do not allow supported Plug and Play device redirection and disable this policy.