Dell Wyse ThinOS Version 8.5 and ThinOS Lite 2.5 Operating System

Release Notes

Notes, cautions, and warnings

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.

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

2019 - 06

Rev. A00

Contents

1

Overview

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

NOTE: For details about the previous versions, if applicable, or to determine which version of the operating system you need to select for your thin client, see Version matrix.

2

Version matrix

The following version matrix lists the platforms supported in each ThinOS release, and helps you select which version of ThinOS software is appropriate for your work environment.

Table 1. Version matrix

Release version	Release date	Supported platforms	Release Notes
ThinOS 8.5_024	December 2018	• Wyse 3010 thin client with ThinOS (T10) • 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 PCoIP • 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 7010 thin client with ThinOS (Z10D)	Release version ThinOS 8.5_024
ThinOS Lite 2.5_024	December 2018	• Wyse 3010 zero client for Citrix • Wyse 3020 zero client for Citrix • Wyse 5010 zero client for Citrix	Release version ThinOS Lite 2.5_024
ThinOS 8.5_115	December 2018	• Wyse 5070 thin client • Wyse 5070 Extended thin client	Release version ThinOS 8.5_115
ThinOS 8.5_113	September 2018	• Wyse 5070 thin client • Wyse 5070 Extended thin client	Release version ThinOS 8.5_113
ThinOS 8.5_020	September 2018	• Wyse 3010 thin client with ThinOS (T10) • 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 PCoIP • 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	Release version ThinOS 8.5_020

Release version	Release date	Supported platforms	Release Notes
		• Wyse 5060 thin client with PCoIP • Wyse 7010 thin client with ThinOS (Z10D)	
ThinOS Lite 2.5_020	September 2018	• Wyse 3010 zero client for Citrix • Wyse 3020 zero client for Citrix • Wyse 5010 zero client for Citrix	Release version ThinOS Lite 2.5_020
ThinOS 8.5_107	June 2018	• Wyse 5070 thin client • Wyse 5070 Extended thin client	Release version ThinOS 8.5_107
ThinOS 8.5_017	June 2018	• Wyse 3010 thin client with ThinOS (T10) • 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 PCoIP • 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 7010 thin client with ThinOS (Z10D)	Release version ThinOS 8.5_017
ThinOS Lite 2.5_017	June 2018	• Wyse 3010 zero client for Citrix • Wyse 3020 zero client for Citrix • Wyse 5010 zero client for Citrix	Release version ThinOS Lite 2.5_017
ThinOS 8.5_012	March 2018	• Wyse 3010 thin client with ThinOS (T10) • 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 PCoIP • 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 7010 thin client with ThinOS (Z10D)	Release version ThinOS 8.5_012
ThinOS Lite 2.5_012	March 2018	• Wyse 3010 zero client for Citrix • Wyse 3020 zero client for Citrix • Wyse 5010 zero client for Citrix	Release version ThinOS Lite 2.5_012

ThinOS 8.5_024 and ThinOS Lite 2.5_024

Priority and recommendations

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

Feature updates

This section contains information about the feature updates.

- VMware Horizon package is updated to version 4.6.51718 to resolve the user trap issue on Blast protocol.
- 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 automatically configured. To load the default settings for DP audio, reset the thin client to factory default settings. However, thin clients that are shipped with the latest version of ThinOS are configured with the default settings. For information about the known issue, see the Known issue section.

NOTE: For more information about ThinOS features, see the *Dell Wyse ThinOS Version 8.5 Hotfix Administrator's Guide* at Dell.com/support.

Supported platforms

Table 2. Supported platforms

Platform	Image file name	BIOS file name
Wyse 3010 thin client with ThinOS—T10	DOVE_boot	Not available
Wyse 3010 zero client for Citrix	T00_xen.bin	Not available
Wyse 3020 thin client with ThinOS—T10D	T10D_wnos	Not available
Wyse 3020 zero client for Citrix	T00D_xen	Not available
Wyse 3030 LT thin client with ThinOS	U10_wnos	U10_bios.bin
Wyse 3030 LT thin client with PCoIP	PU10_wnos	PU10_bios.bin
Wyse 3040 thin client with ThinOS	A10Q_wnos	A10Q_bios.bin
Wyse 3040 thin client with PCoIP	PA10Q_wnos	A10Q_bios.bin
Wyse 5010 thin client with ThinOS—D10D	ZD10_wnos	D10G_bios.bin
Wyse 5010 thin client with PCoIP—D10DP	PD10_wnos	PD10G_bios.bin
Wyse 5010 zero client for Citrix	ZD00_xen	ZD00_bios.bin
Wyse 5040 AIO thin client—5212	ZD10_wnos	AIO10G_bios.bin
Wyse 5040 AIO thin client with PCoIP—5213	PD10_wnos	PAIO10G_bios.bin
Wyse 5060 thin client with ThinOS	D10Q_wnos	D10Q_bios.bin

Platform	Image file name	BIOS file name
Wyse 5060 thin client with PCoIP	PD10Q_wnos	PD10Q_bios.bin
Wyse 7010 thin client with ThinOS—Z10D	ZD10_wnos	Z10G_bios.bin

Packages

The following table provides the list of the packages that are available:

Table 3. Packages

Package name	Version
FR	1.20.46089
Horizon	4.6.51718
RTME	2.4.48792
TCX	7.1.41853

Tested environment

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

Table 4. Test environment - General components

Component	Version
Wyse Management Suite	1.2
Wyse Device Manager	5.7.3
Imprivata OneSign	5.5
Caradigm	6.3.1
NetScaler	11.1/12.0
StoreFront	3.12
Web Interface	5.4
SecureMatrix	4.1.0

Table 5. Test environment - VDI components

	Windows 7	Windows 10	Linux	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Application
VMware Horizon 7.0	√	√	√	√	√	√	√
Citrix Virtual Apps and Desktops (formerly XenDesktop) 5.6	√	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Citrix Virtual Apps (formerly XenApp) 6.5	Not applicable			√	Not applicable		√

	Windows 7	Windows 10	Linux	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Application
Citrix Virtual Apps and Desktops 7.15 and Citrix Virtual Apps 7.15	√	√		√	√	√	√
Tera PCM for Amazon WorkSpaces 1.03	√ *	Not applicable		Not applicable	Not applicable	Not applicable	Not applicable
Microsoft Remote Desktop Services (RDS) 2012 R2 and RDS 2016	√	√			√	√	√

*Amazon WorkSpace VM operating system—Windows 7 style—is based on 2008 R2 RDSH.

Table 6. Test environment - Citrix Virtual Apps and Desktops

Citrix Virtual Apps and Desktops/Citrix Virtual Apps	Operating system	Citrix RealTime Media Engine (RTME)	Lync client	Skype for Business (SFB) server
7.15	Windows 7	2.4	Skype For Business 2016	Skype For Business 2015
	Windows 10	2.4	Skype For Business 2016	Skype For Business 2015
	Windows Server 2016	2.4	Skype For Business 2016	Skype For Business 2015

Fixed issues

The following table provides the list of fixed issues in this release:

Table 7. Fixed issues

Issue number	Description
TIR97721	Resolved the client trap issue that occurs when the on-board audio from BIOS is disabled on the Wyse 5010 thin client.
TIR96954	Resolved an issue where keyboard and mouse input are lost when you use multiport ICA and UDP audio.
TIR97799	SCEP functionality is enhanced to work without an enrollment password.
TIR97768	Resolved an issue where the order of audio devices is not continuous on the Wyse 3040 thin client.
TIR97194	Resolved an issue where all cached illustrations are displayed instead of the selected illustrations when you set the INI parameter `screensaver type=3`.
TIR97031	Resolved an issue where the **Packages** tab is not displayed in **System Tools** when you convert a thin client running another operating system to ThinOS by using Dell Wyse USB Imaging Tool version 3.1 on the Wyse 5070 thin client.
TIR97786	Resolved an issue where a built-in certificate expired message is displayed in **Event Log** when you boot the device.
TIR97818	Reliability of RTMediaEngineSrv—out of system heap is improved.
TIR97767	Resolved an issue where the display artifacts are displayed in the RDP session.

Issue number	Description
TIR97872	Resolved an issue where importing a root certificate fails.
TIR97723/TIR96094	Stability is improved to avoid the Trap Error 14 in the Blast session.
TIR98003	Audio quality is improved in the RDP session.
TIR98172	Resolved a DaaS issue where the **Connection tunnel failed** message is displayed during two-factor authentication.
TIR97897	Resolved an issue where an active Server Name Indication (SNI) displays the **SSL: error ERR_SSL_NO_CIPHER_MATCH** error message.
TIR97820	Resolved an issue where SCEP renewal occurs during the system bootup.
TIR97763	Resolved a smart card issue related to secure messaging mode.
TIR98325	Resolved an issue where the Numlock LED status is turned off after you disconnect from a VDI desktop in the Blast session.
TIR98318	Resolved a Citrix NetScaler two-factor authentication log in issue where the incorrect session cookie is removed when the Storefront server FQDN is same as the NetScaler FQDN.
TIR97783	Resolved an issue where CAC smart card users are not able to select the token that is used to log in to VMware Horizon session.
TIR97651	Resolved an issue where the wireless association fails when the beacon lost events occur on the Wyse 5040 AIO thin client.
TIR98442	Resolved the German language alignment issue by enhancing the OpenVPN User Interface text.
TIR98316	Resolved an issue where the DNS resolution results in Citrix sign-on failure.
TIR96546	DisplayPort Audio option is disabled by default.
TIR95973/TIR97650	Resolved an issue where display does not wake up from sleep mode on the Wyse 3040 thin client.
TIR97803	Resolved an issue where access points are not displayed on the Wyse 3040 thin client while roaming.
TIR96801	Resolved a check-in issue in Wyse Device Manager where the thin client stops working.
TIR98197	Resolved an issue where multiple certificate CN= entries result in Sign-on failure.
TIR98044	Resolved an issue where a certificate `TLSCheckCN=no` is not recognized.
TIR96944	Resolved an issue where Internet Explorer 11 fields stop responding in the RDP session on firmware later than version 8.4_009.
TIR97734	Resolved an issue where the location-based printers are not mapped correctly.
TIR97323	Resolved an issue where the cursor is invisible when you use Solidworks and Adobe Reader applications in the ICA session.
TIR96913	Resolved an issue where the display information is not registered in the ThinOS Event Log or Device Manager.
TIR96608	Resolved a memory leak issue that results in screen overlaying after multiple sessions are launched.
TIR97978	The domain\username format is added in the **SignOn username** field.
TIR98298	General client stability is improved.
TIR98414	Reduced the failover time delay when you use high availability in Imprivata.
TIR97484	Resolved an issue where ThinOS sends an RDP session message before you login.
TIR98114	Resolved an issue where Admin CAC smart card does not prompt you to enter the PIN.

Issue number	Description
TIR96236	Improved the session reconnection period when using the VMware Horizon client.
TIR97153	Resolved an issue where the data cannot be copied to a USB drive on the Wyse 3020 thin client.
TIR98539	Resolved an issue where a single enumerated session does not automatically launch in the VMware Horizon client.
TIR98537	Resolved an issue where the `OnDesktop` parameter is not recognized in the zero launch bar (VDI) mode.
TIR98517	Resolved a connection issue where the HTTP header keyword **Content-Length** is returned by Citrix Netscaler as **Cteonnt-Length**.
TIR98195	Resolved an issue where the touch screen tab is disabled.
TIR98491	Resolved an issue where **Failed To Set Admin Password** message is displayed in **Event Log** after you change the BIOS password.

Known issue

This section describes the known issue in this release.

Table 8. Known issue

Issue number	Description	Workaround
TIR94278	On Wyse 3040 thin client, if you set the display resolution higher than 1920 X 1080, and enable the DisplayPort audio, a black screen is displayed for 10 seconds after the system reboot. DP audio stops responding when the black screen issue is observed	Do not enable the DisplayPort audio. By default, DP audio is disabled on Wyse 3040 thin client.

4

ThinOS 8.5_115

Priority and recommendations

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

Feature updates

This section contains information about the feature updates.

- VMware Horizon package is updated to version 4.6.51718 to resolve the user trap issue on Blast protocol.
- UI enhancement that enables you to restart the client immediately or delay the restart when Wyse Management Suite policy changes need to be applied to ThinOS.
- Changes to display priority on Wyse 5070 Extended thin client to support the latest AMD BIOS firmware. The display priority is as follows:
  - 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

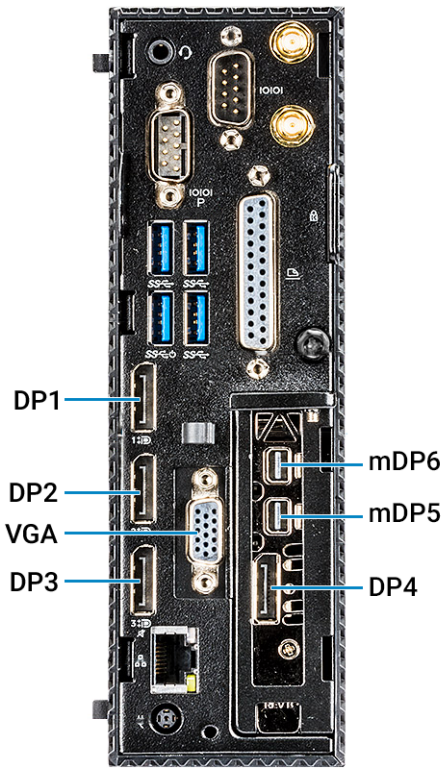

Figure 1. Display priority

NOTE: For more information about ThinOS features, see the *Dell Wyse ThinOS Version 8.5.1 Administrator's Guide* at Dell.com/support.

Supported platforms

Table 9. Supported platforms

Platform	Image file name	BIOS file name
Wyse 5070 thin client with ThinOS	X10_wnos	X10_bios.bin
Wyse 5070 thin client with PCoIP	PX10_wnos	X10_bios.bin

Packages

The following table provides the list of the packages that are available:

Table 10. Packages

Package name	Version
FR	1.20.46089
Horizon	4.6.51718
RTME	2.4.48792
TCX	7.1.41853

Tested environment

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

Table 11. Test environment - General components

Component	Version
Wyse Management Suite	1.2
Wyse Device Manager	5.7.3
Imprivata OneSign	5.5
Caradigm	6.3.1
NetScaler	11.1/12.0
StoreFront	3.12
Web Interface	5.4
SecureMatrix	4.1.0

Table 12. Test environment - VDI components

	Windows 7	Windows 10	Linux	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Application
VMware Horizon 7.0	√	√	√	√	√	√	√
Citrix Virtual Apps and Desktops (formerly XenDesktop) 5.6	√	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Citrix Virtual Apps (formerly XenApp) 6.5	Not applicable			√	Not applicable		√
Citrix Virtual Apps and Desktops 7.15 and Citrix Virtual Apps 7.15	√	√		√	√	√	√
Tera PCM for Amazon WorkSpaces 1.03	√ *	Not applicable		Not applicable	Not applicable	Not applicable	Not applicable
Microsoft Remote Desktop Services	√	√			√	√	√

	Windows 7	Windows 10	Linux	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Application
(RDS) 2012 R2 and RDS 2016							

*Amazon WorkSpace VM operating system—Windows 7 style—is based on 2008 R2 RDSH.

Table 13. Test environment - Citrix Virtual Apps and Desktops

Citrix Virtual Apps and Desktops/Citrix Virtual Apps	Operating system	Citrix RealTime Media Engine (RTME)	Lync client	Skype for Business (SFB) server
7.15	Windows 7	2.4	Skype For Business 2016	Skype For Business 2015
	Windows 10	2.4	Skype For Business 2016	Skype For Business 2015
	Windows Server 2016	2.4	Skype For Business 2016	Skype For Business 2015

Fixed issues

The following table provides the list of fixed issues in this release:

Table 14. Fixed issues

Issue number	Description
TIR97721	Resolved the client trap issue that occurs when the on-board audio from BIOS is disabled on the Wyse 5010 thin client.
TIR96954	Resolved an issue where keyboard and mouse input are lost when you use multiport ICA and UDP audio.
TIR97799	SCEP functionality is enhanced to work without an enrollment password.
TIR97768	Resolved an issue where the order of audio devices is not continuous on the Wyse 3040 thin client.
TIR97194	Resolved an issue where all cached illustrations are displayed instead of the selected illustrations when you set the INI parameter `screensaver type=3`.
TIR97031	Resolved an issue where the **Packages** tab is not displayed in **System Tools** when you convert a thin client running another operating system to ThinOS by using Dell Wyse USB Imaging Tool version 3.1 on the Wyse 5070 thin client.
TIR97786	Resolved an issue where a built-in certificate expired message is displayed in **Event Log** when you boot the device.
TIR97818	Reliability of RTMediaEngineSrv—out of system heap is improved.
TIR97767	Resolved an issue where the display artifacts are displayed in the RDP session.
TIR97872	Resolved an issue where importing a root certificate fails.
TIR97723/TIR96094	Stability is improved to avoid the Trap Error 14 in the Blast session.
TIR98003	Audio quality is improved in the RDP session.
TIR98172	Resolved a DaaS issue where the **Connection tunnel failed** message is displayed during two-factor authentication.
TIR97897	Resolved an issue where an active Server Name Indication (SNI) displays the **SSL: error ERR_SSL_NO_CIPHER_MATCH** error message.

Issue number	Description
TIR97820	Resolved an issue where SCEP renewal occurs during the system bootup.
TIR97763	Resolved a smart card issue related to secure messaging mode.
TIR98325	Resolved an issue where the Numlock LED status is turned off after you disconnect from a VDI desktop in the Blast session.
TIR98318	Resolved a Citrix NetScaler two-factor authentication log in issue where the incorrect session cookie is removed when the Storefront server FQDN is same as the NetScaler FQDN.
TIR97783	Resolved an issue where CAC smart card users are not able to select the token that is used to log in to VMware Horizon session.
TIR97651	Resolved an issue where the wireless association fails when the beacon lost events occur on the Wyse 5040 AIO thin client.
TIR98442	Resolved the German language alignment issue by enhancing the OpenVPN User Interface text.
TIR98316	Resolved an issue where the DNS resolution results in Citrix sign-on failure.
TIR96546	DisplayPort Audio option is disabled by default.
TIR95973/TIR97650	Resolved an issue where display does not wake up from sleep mode on the Wyse 3040 thin client.
TIR97803	Resolved an issue where access points are not displayed on the Wyse 3040 thin client while roaming.
TIR96801	Resolved a check-in issue in Wyse Device Manager where the thin client stops working.
TIR98197	Resolved an issue where multiple certificate CN= entries result in Sign-on failure.
TIR98044	Resolved an issue where a certificate `TLSCheckCN=no` is not recognized.
TIR96944	Resolved an issue where Internet Explorer 11 fields stop responding in the RDP session on firmware later than version 8.4_009.
TIR97734	Resolved an issue where the location-based printers are not mapped correctly.
TIR97323	Resolved an issue where the cursor is invisible when you use Solidworks and Adobe Reader applications in the ICA session.
TIR96913	Resolved an issue where the display information is not registered in the ThinOS Event Log or Device Manager.
TIR96608	Resolved a memory leak issue that results in screen overlaying after multiple sessions are launched.
TIR97978	The domain\username format is added in the **SignOn username** field.
TIR98298	General client stability is improved.
TIR98414	Reduced the failover time delay when you use high availability in Imprivata.
TIR97484	Resolved an issue where ThinOS sends an RDP session message before you login.
TIR98114	Resolved an issue where Admin CAC smart card does not prompt you to enter the PIN.
TIR96236	Improved the session reconnection period when using the VMware Horizon client.
TIR97153	Resolved an issue where the data cannot be copied to a USB drive on the Wyse 3020 thin client.
TIR98539	Resolved an issue where a single enumerated session does not automatically launch in the VMware Horizon client.
TIR98537	Resolved an issue where the `OnDesktop` parameter is not recognized in the zero launch bar (VDI) mode.
TIR98517	Resolved a connection issue where the HTTP header keyword **Content-Length** is returned by Citrix Netscaler as **Cteonnt-Length**.
TIR98195	Resolved an issue where the touch screen tab is disabled.

Issue number	Description
TIR98491	Resolved an issue where **Failed To Set Admin Password** message is displayed in **Event Log** after you change the BIOS password.

ThinOS 8.5_113

Priority and recommendations

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

Feature updates

- Dell Wyse 5070 thin clients with ThinOS version 8.5_113 are IPv6-certified.
- Dell Wyse 5070 thin clients with ThinOS version 8.5_113 are ENERGY STAR compliant.

NOTE:

- For more information about the ThinOS features, see the Dell Wyse ThinOS Version 8.5.1 Administrator's Guide at Dell.com/support.
- For more information about the newly added parameters, see the latest Dell Wyse ThinOS Version 8.5.1 INI Reference Guide at Dell.com/support.

Supported platforms

Table 1 describes the supported platforms and associated firmware in this release.

Table 15. Supported platforms

Platform	ThinOS	ThinOS with PCoIP
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

BIOS information

Table 2 describes the latest BIOS information in this release.

Table 16. BIOS information

Platform	BIOS version	BIOS BIN file name—for ThinOS update
Wyse 5070 thin client—Celeron	Dell BIOS 1.1.1	X10_bios.bin
Wyse 5070 thin client—Pentium	Dell BIOS 1.1.1	X10_bios.bin
Wyse 5070 Extended thin client	Dell BIOS 1.1.1	X10_bios.bin

Known issues

None

Fixed issues

This section describes the fixed issues in this release.

Table 17. Fixed issues

Issue number	Issue description
TIR94834	After reboot, you cannot reconnect the Bluetooth headsets, and you must reboot headsets to reconnect. This functionality works as designed by Intel.
TIR96293	SessionConfig=RDP, GracefulReconnTimeout=xx If you connect to RDP Windows 10 without the RemoteFX session and enable H.264-AVC444, this ini parameter causes the session to autodisconnect and reconnect frequently. The thin client decoder may fail after several attempts to reconnect. After the thin client decoder fails and the main screen goes to sleep or you turn off the main screen, the session is launched on the second screen automatically. However, the trap **winmgr** is observed.
TIR95276	When you modify the thin client preferences, the thin client resets to the factory default settings and a black screen is displayed.
TIR96028	When you connect two monitors on DP1 and DP2 and extend the displays across the monitors, the DP audio does not work.

6

ThinOS 8.5_107

Priority and recommendations

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

New features

This section contains new features in this release.

Wireless chipset—Intel Dual Band Wireless AC 9560

Wyse 5070 thin client supports new wireless chipset Intel Dual Band Wireless AC 9560. The wireless and Bluetooth features are similar to ThinOS 8.5.0.

For the list of known issues about the wireless chipset, see Known issues.

Dual Network Interface

Wyse 5070 thin client supports an optional module—RJ45/SFP. If you use an optional RJ45 or SFP module, dual NIC is enabled and the wireless connection is disabled. In the **Network Setup** window, the dual network interface options are displayed—ENET0 and ENET1.

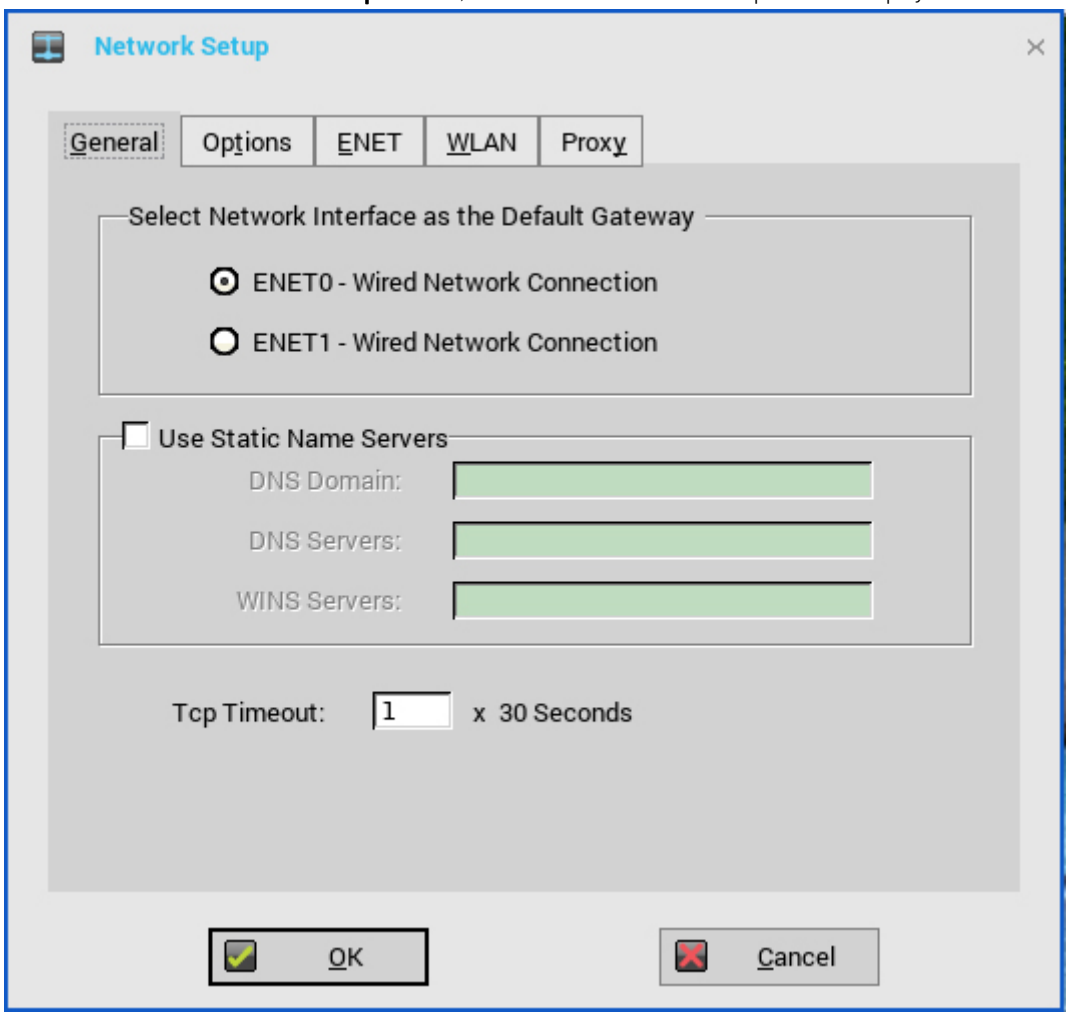

Figure 2. Network Setup

In the **ENET** tab, from the **Ethernet Select** drop-down list, select ENET0 or ENET1 to configure the corresponding Ethernet connection settings.

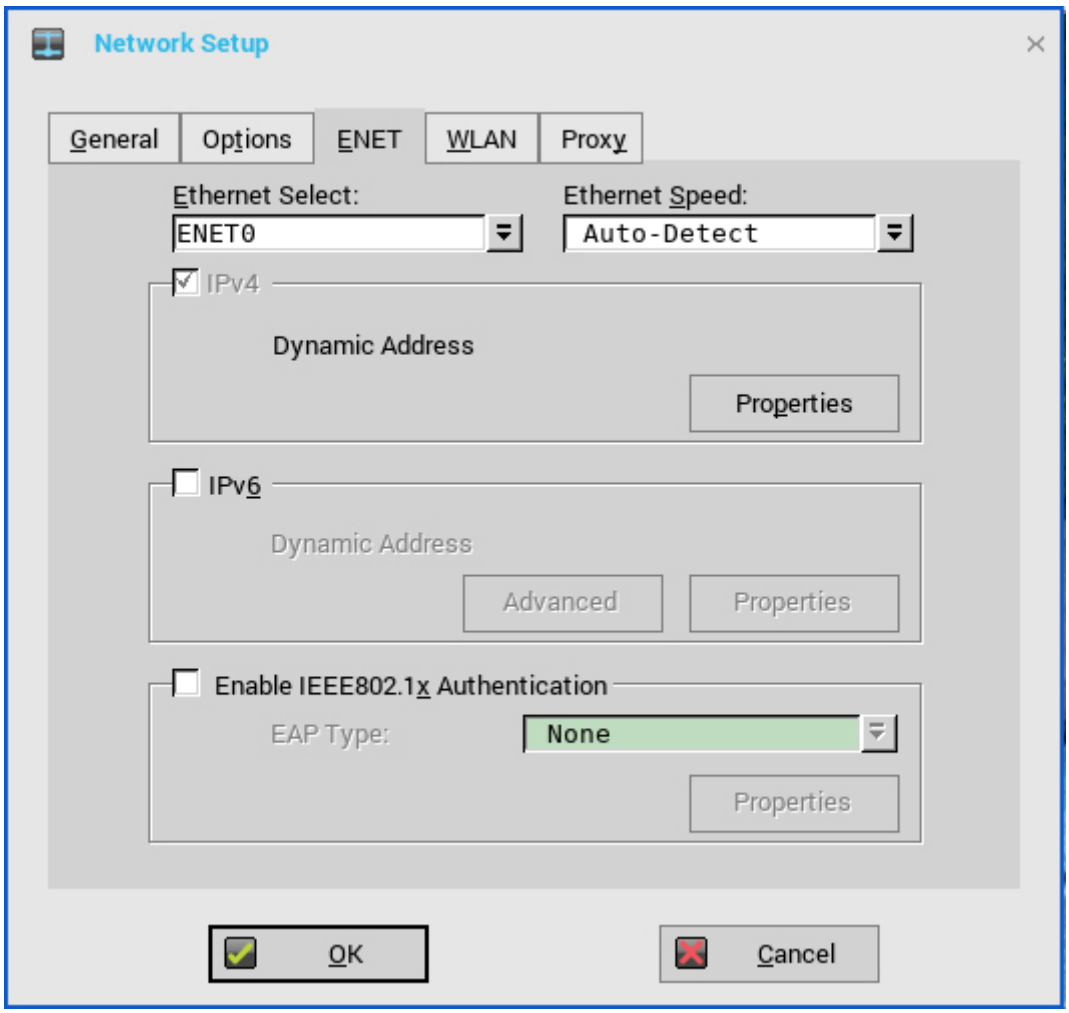

Figure 3. ENET

In the **System Information** window, the ENET tab is modified as displayed in the following screenshot:

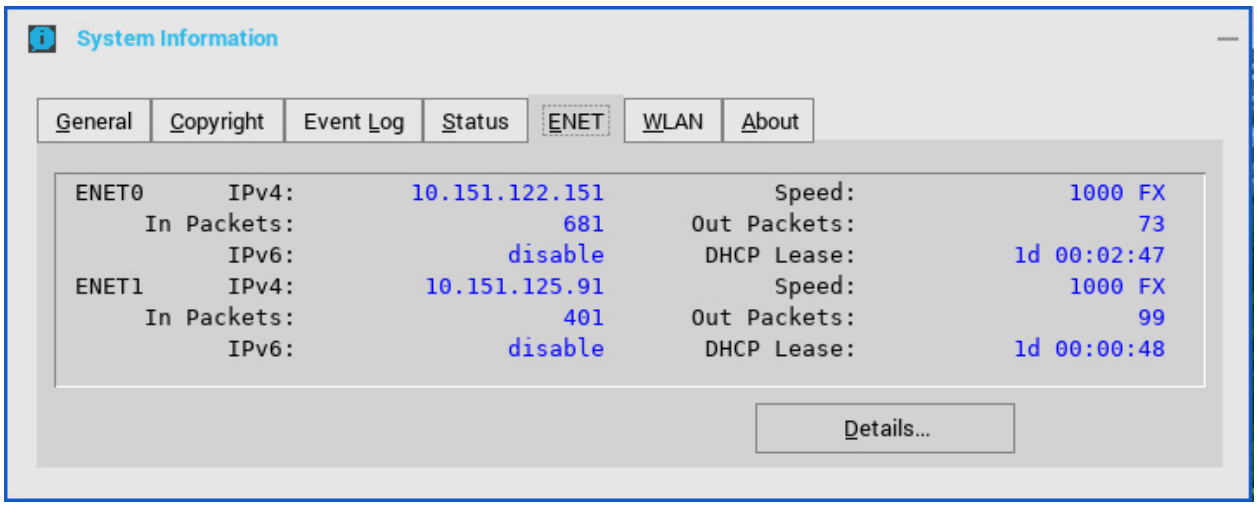

Figure 4. System Information

To view all the network information, click **Details**.

Figure 5. Details

For the list of known issues about the Dual Network Interface (NIC), see Known issues.

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 inside TPM—**TPM_PCR16**. This is used to generate disk encryption/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

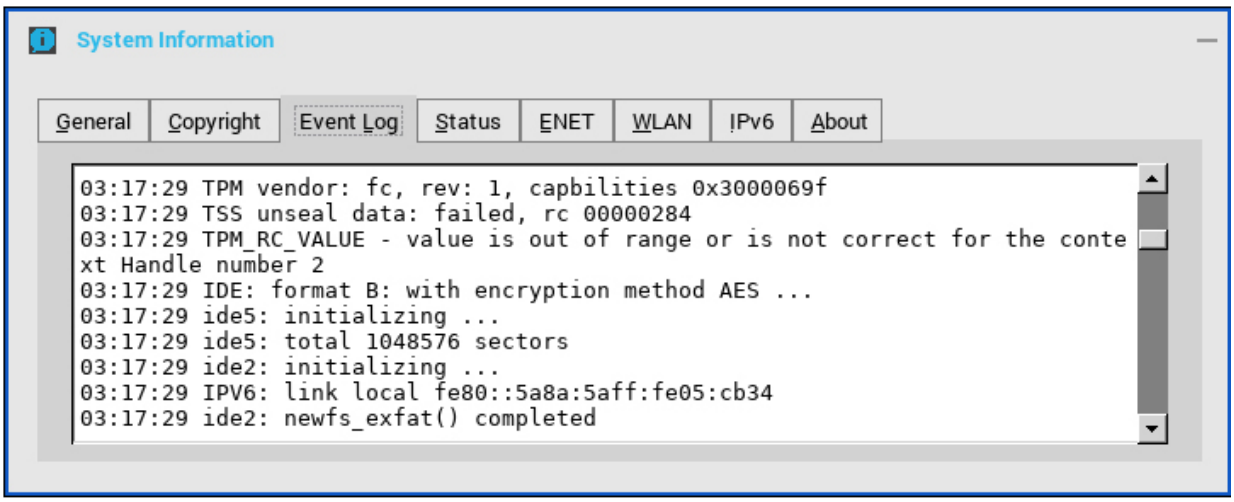

Figure 6. Event Log

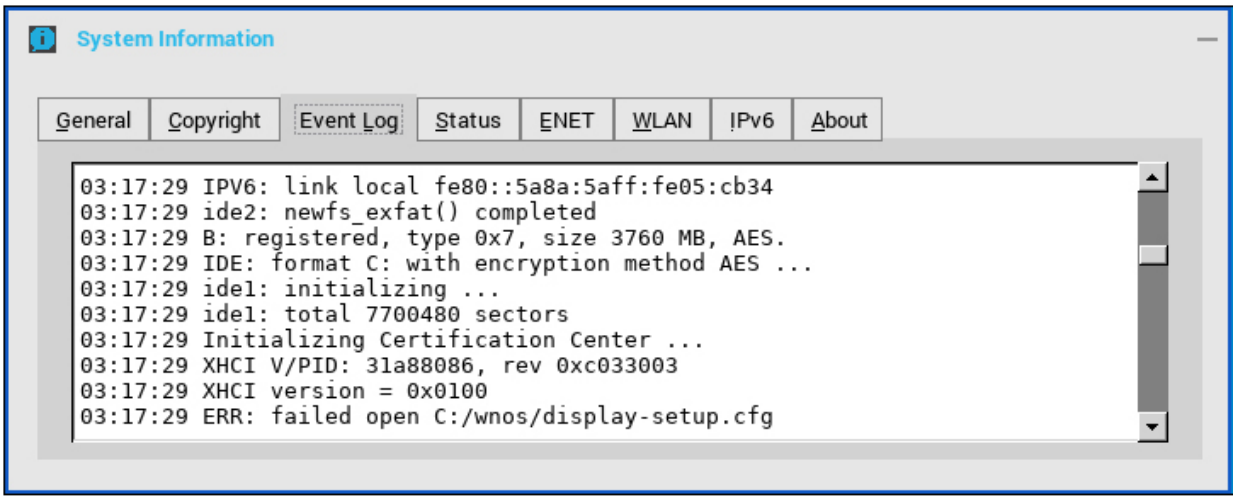

Figure 7. Event Log

– 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.

Mouse settings

To access the mouse setting, go to **System Setup** > **Peripherals** and select **Mouse**. The following two options are introduced in the mouse setting:

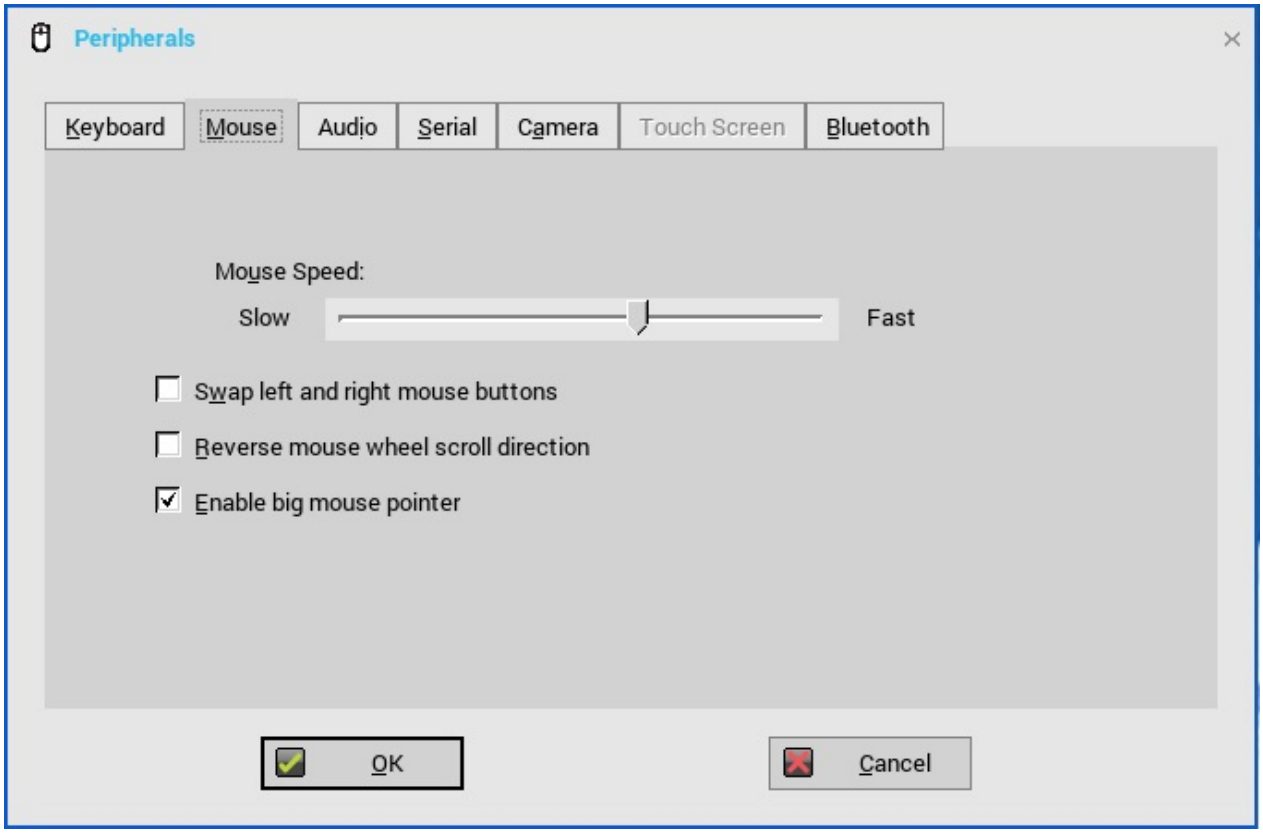

Figure 8. Mouse settings

- Reverse mouse wheel scroll direction—Select the **Reverse mouse wheel scroll direction** check box to invert the direction of the mouse scroll wheel. A new INI parameter **FlipFlopWheel** is introduced. For more information about the INI parameter, see INI parameters.
- Enable big mouse pointer—Select the **Enable big mouse pointer** check box to increase the size of the local mouse pointer by two times. A new INI parameter **Big** is introduced. For more information about the INI parameter, see INI parameters.

NOTE: This option affects ThinOS local mouse pointer.

Display setup

The multi-display setup is a new feature introduced in ThinOS 8.5.1 release to support multiple monitors. Use the **Display Setup** dialog box to configure the display settings for the connected monitors.
To configure the display setup:

1 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:

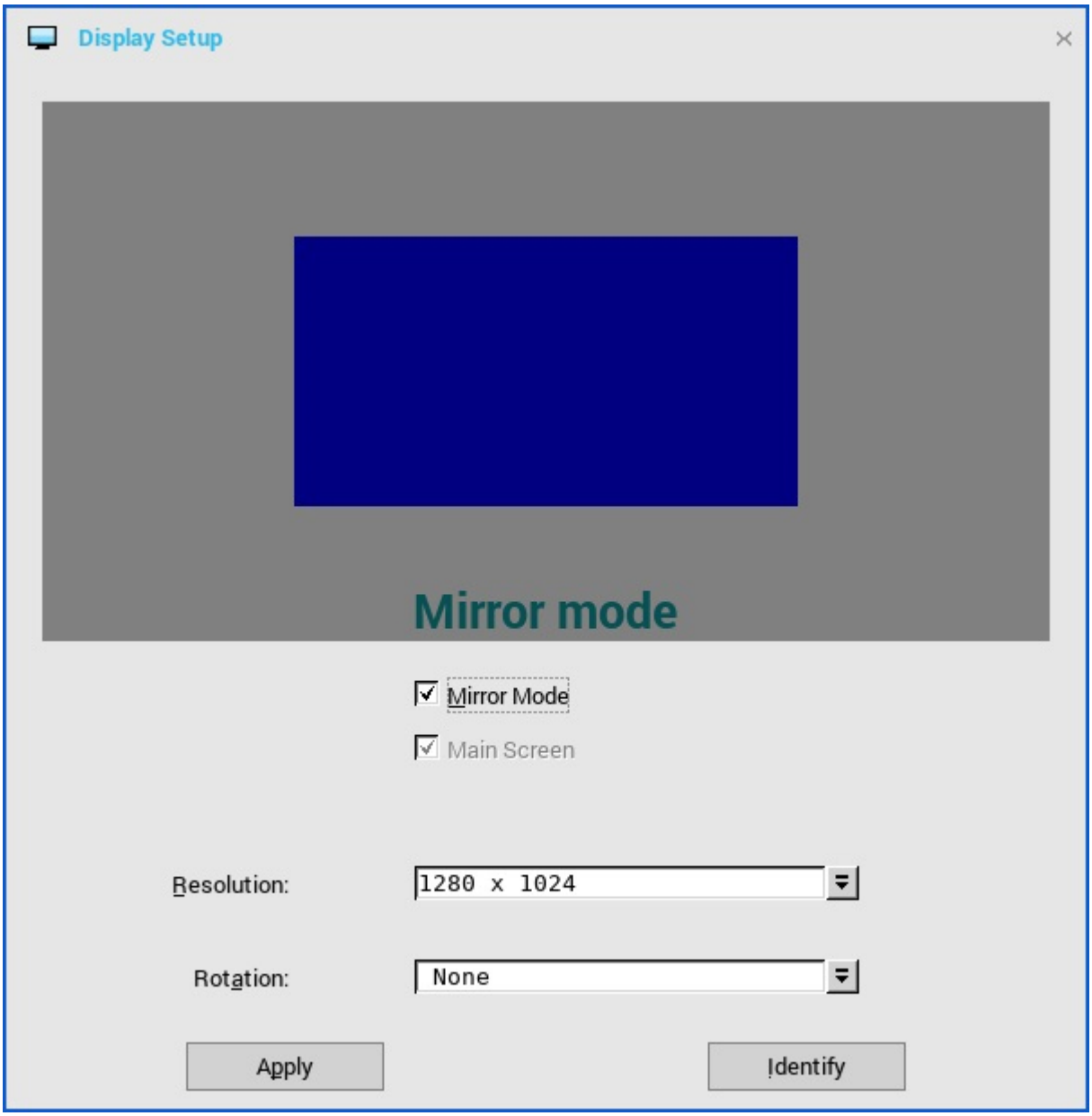

Figure 9. Mirror mode

If you clear the **Mirror mode** check box, the **Span Mode** is enabled. The following screen represents the span mode configuration:

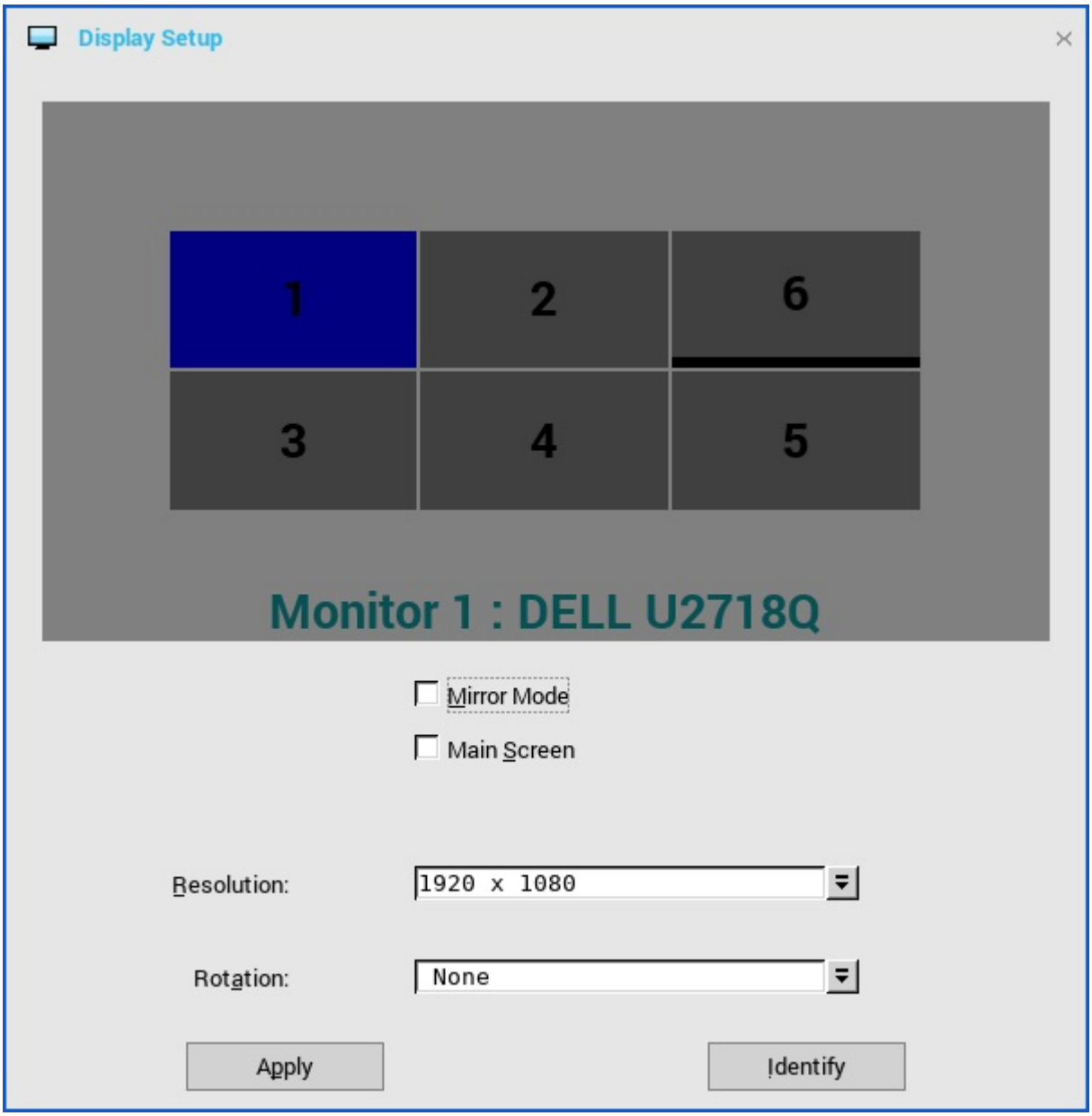

Figure 10. Span mode

Blocks displayed on the screen represent the number of monitor screens connected to 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.

NOTE: Wyse 5070 thin client supports up to six monitors.

- **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 the 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.

NOTE: Main screen option is effective only in Span Mode and always it is disabled in Mirror Mode.

- **Resolution**—From the **Resolution** drop-down list, select a display resolution supported by your monitor.

  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 see the modified display.

4 Click **OK** to confirm the new settings.

NOTE: Use the Identify option, to know the display order number of the connected monitors.

For the list of known issues about the display setup, see Known issues.

NOTE: You can configure the multi-display setup manually. If you want to set automatic configurations for multi-display setup using INI, use the Dual head parameters. You can define the behavior of the first two monitors using INI parameters, and the remaining monitors follow the settings configured for the first two monitors.

Hardware capability

This section describes the hardware capability for display.

Table 18. Port preferences

Platform	Port preferences
Wyse 5070 thin client with Celeron processor	• On Wyse 5070 thin client without wireless module, the optional port can be used as second RJ-45, SFP, VGA, or second serial port. • On Wyse 5070 thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP. • When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive.
Wyse 5070 thin client with Pentium processor	• On Wyse 5070 thin client without wireless module, the optional port can be used as second RJ-45, SFP, VGA, or second serial port. • On Wyse 5070 thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP. • Back headset is disabled if front headphone is used. • When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive. • When VGA monitor is connected on VGA optional port, DisplayPort 3 becomes inactive.
Wyse 5070 Extended thin client	• On Wyse 5070 Extended thin client without wireless module, the optional port can be used as second RJ-45, SFP, or VGA. • On Wyse 5070 Extended thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP. • Back headset is disabled if front headphone is used. • When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive. • When VGA monitor is connected on VGA optional port, DisplayPort 3 becomes inactive. • Power option is available on the first serial port. • PCIe slot is available.

Wyse 5070 thin client with Pentium processor

Table 19. Display matrix

Number of displays	Supported display resolution	
	4K resolution 3840 x 2160 @ 60 Hz	Non-4K resolution Up to 2560 x 1600 @ 60 Hz
One display	Yes	Yes
Two displays	Yes	Yes
Three displays[1]	Yes	Yes

[1]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 20. Ports

Ports	DP1	DP2	DP3	VGA	USB Type-C
Monitor priority	1	2B[1]	3B[2]	3A[2]	2A[1]
4K display	Yes	Yes	Yes	No[3]	Yes
Non-4K display	Yes	Yes	Yes	Yes[3]	Yes

[1]DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

[2]DP3 and VGA port are mutually exclusive with VGA port taking higher priority.

[3]VGA port supports only 1080p resolution.

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 Celeron processor

Table 21. Display matrix

Number of displays	Supported display resolution	
	4K resolution 3840 x 2160 @ 60 Hz	Non-4K resolution Up to 2560 x 1600 @ 60 Hz
One display	Yes	Yes
Two displays	Yes	Yes
Three displays	No[1]	Yes[2]

[1]VGA port does not support 4K display. However, it supports a display with 1080p screen resolution.

[2]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 22. Ports

Ports	DP1	DP2	VGA	USB Type-C
Monitor priority	1	2B[1]	3	2A[1]
4K display	Yes	Yes	No[2]	Yes

Ports	DP1	DP2	VGA	USB Type-C
Non-4K display	Yes	Yes	Yes[2]	Yes

[1]DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

[2]VGA port supports only 1080p resolution.

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 23. Wyse 5070 Extended thin client with AMD GPU

Number of displays	Supported display resolution	
	4K resolution 3840 x 2160 @ 60 Hz	Non-4K resolution Up to 2560 x 1600 @ 60 Hz
One display	Yes	Yes
Two displays	Yes	Yes
Three displays[1]	Yes	Yes
Four displays[2]	Yes	Yes
Five displays[2]	Yes	Yes
Six displays[2]	Yes[2]	Yes

[1]Dell recommends that you configure first two 4K displays on the main board (DP1~DP3), and the third 4K display on AMD GPU card.

[2]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.

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 24. Ports

Ports	DP1	DP2	DP3	VGA	USB Type-C	mDP4	mDP5	DP6
Monitor priority	1	2B[1]	3B[2]	3A[2]	2A[1]	4	5	6
4K display	Yes	Yes	Yes	No[3]	Yes	Yes	Yes	Yes
Non-4K display	Yes	Yes	Yes	Yes[3]	Yes	Yes	Yes	Yes

[1]DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

[2]DP3 and VGA port are mutually exclusive with VGA port taking higher priority.

[3]VGA port supports only 1080p resolution.

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.

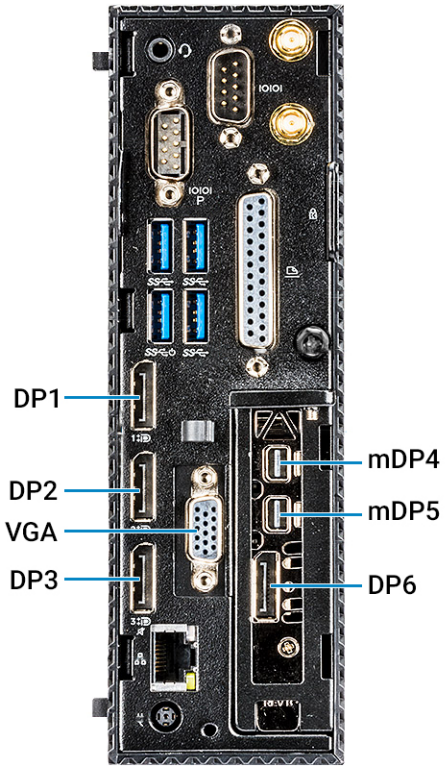

Figure 11. Ports on Wyse 5070 Extended thin client

Monitor priority—The following order defines the monitor priority set on ThinOS for Wyse 5070 Extended thin client:

- DP1 > DP2 > DP3 > mDP4 > mDP5 > DP6
- DP1 > USB Type-C > DP3 > mDP4 > mDP5 > DP6
- DP1 > DP2 > VGA > mDP4 > mDP5 > DP6
- DP1 > USB Type-C > VGA > mDP4 > mDP5 > DP6

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.

INI parameters—The INI parameters for display in Wyse 5070 thin client are from ThinOS 8.5 legacy INI. The INI parameter supports only two monitors, that is, the INI settings can only impact the first two screens. If you add the third screen, it follows the display settings defined for the second screen. There are few settings that are not applicable for Wyse 5070 thin client with ThinOS. For more information, see INI parameters. Further solution on INI settings for Wyse 5070 thin client with ThinOS is provided post RTS.

Multi-monitors support for different protocols

This section contains information about using multiple monitors on different protocols.

Support for multi-monitors in Citrix

ThinOS supports ICA desktop multiple monitors in XenDesktop/XenApp 7.6 and later.
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 at 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 25. Display details

Platforms	Best 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—Pentium processor	1920 x 1080	3	3
	2560 x 1440	3	3
	3840 x 2160	3	Not supported, due to GRID K1/K2 vGPU profile limitation.
Wyse 5070 thin client—Celeron processor	1920 x 1080	2	2
	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 are supported.
- For HDX 3D Pro desktop using vGPU or GPU Passthrough, the supported resolution and number of supported monitors are dependent 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.

Support for multi-monitors in VMware Blast session

ThinOS supports multiple-monitor display to run virtual machines on each monitor.
Update the VMware Blast package to the latest version. The Horizon package version is 4.6.47369.
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 a full screen VMware Horizon Blast session.

- **Display numbers**—Virtual machine needs sufficient video memory to support multiple monitors. You can use up to four monitors with sufficient RAM.

Table 26. Display matrix

	Resolution	1920 x 1080					2560 x 1440				
Display layout	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

- **4K display**—With the VMware Blast display protocol a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

Table 27. 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 28. 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.
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.

Support for multi-monitors in PCoIP

ThinOS supports multiple-monitor display to run virtual machines 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 a full screen PCoIP session.

- **Display numbers**—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.
  - Support 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 same screen resolution.
- **Display layout**—Monitors layout 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 29. Matrix for multi screen support

PCoIP Multi-monitor support																
Wyse 5070 Extended thin client																
Display layout	Resolution	1920 x 1200					2560 x 1440					3840 x 2160				
	No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
	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 5070 thin client—Pentium																
Display layout	Resolution	1920 x 1200					2560 x 1440					3840 x 2160				
	No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
	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 5070 thin client—Celeron																
Display layout	Resolution	1920 x 1200					2560 x 1440					3840 x 2160				
	No. of displays	Two	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

Support for multi-monitors in RDP

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.

Table 30. RDP display capability matrix

Destination end point	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 2008 R2	4096 (w) x 2048 (h)	4096 (w) x 2048 (h)
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

Table 31. RDP H.264 decoding matrix

Unit type	GPU	Session	Windows 10/Windows Server 2016		Windows 8.1/Windows Server 2012 R2	
		Display resolution	H.264-AVC444	Decoding	H.264	Decoding
Wyse 5070 Extended thin client—Pentium processor	AMD	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
	Intel	3840 x 2160	Enabled	Software	Disabled	
		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Software
		1920 x 1200	Enabled	Software	Enabled	Hardware
Wyse 5070 thin client—Pentium and Celeron processor	Intel	3840x2160	Enabled	Software	Disabled	
		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Software
		1920 x 1200	Enabled	Software	Enabled	Hardware

NOTE:

- Windows 10/Window Server 2016 with H.264-AVC444 must be hosted in Microsoft RDS 2016 broker.
- Data is based on virtual machine without RemoteFX/vGPU enabled configuration.
- H.264 logs and H.264-AVC444 logs are hidden and not displayed in the **Event Log** tab.

For the list of known issues about the display in RDP, see Known issues.

NOTE: In an RDP session with VOR enabled by default (Windows 8.1 x86), 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. As a workaround, you must reduce the number of monitors or lower the resolutions or switch to other 64-bit operating system with more RAM.

Support for USB Type-C

Wyse 5070 thin client supports USB Type-C port.

- USB 3.1 Type-C connector can be used to perform the following activities:
  - Data transfer—USB mass storage
  - Connect monitors

    NOTE: If you use USB Type-C, one monitor capability is reduced from rear panel, and DP2 is disabled.
  - Charge smartphones
  - Connect USB 2.0, 3.0, and 3.1 compatible devices.
- USB 3.1 Type-C cannot be used for the following:
  - Thunderbolt, HDMI, and MHL alt modes
  - Docking station
  - 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.

Security INI parameter

The default value change of INI parameter **TLSCheckCN** impacts Microsoft broker.

SecurityPolicy=Full; TLSCheckCN=yes/no,

In previous release, the default value of **TLSCheckCN** is no, that means, the SSL connection verified the server identity certificates. You can enter either IP address or FQDN to log in to Microsoft broker.

From ThinOS 8.5.1, the default value of **TLSCheckCN** is yes. By default, the server certificate common name is verified. For instance, if your server identity certificates use FQDN, then you must enter FQDN of Microsoft broker to log in.

If INI parameter is not set, then by default the server identity certificates is verified. If you want to log in to broker using both IP and FQDN, you can set the ini as SecurityPolicy=Full; TLSCheckCN=no.

For the value of head parameter **SecurityPolicy**, the Microsoft RDS brokers always work as full security mode in SSL connection. The security mode is set to full mode during the connection and it does not change if you set the parameter **SecurityPolicy** to any value.

DisplayPort audio

DisplayPort audio is supported on DP1 and DP2.

- To enable the DisplayPort audio on ThinOS:
  a. Set up a monitor with DP audio support.
  b. Connect the ThinOS client to monitor using DP cable.
  c. Plug the analog headset into the monitor DP audio interface.
  d. On the ThinOS desktop, click **System Setup** > **Peripherals** > **Audio** > **Playback devices**, and select the **Enable DP audio** check box.
  e. Start either an RDP, ICA, PCoIP, or Blast session.

f Play a video, and check the audio output using the analog headset.

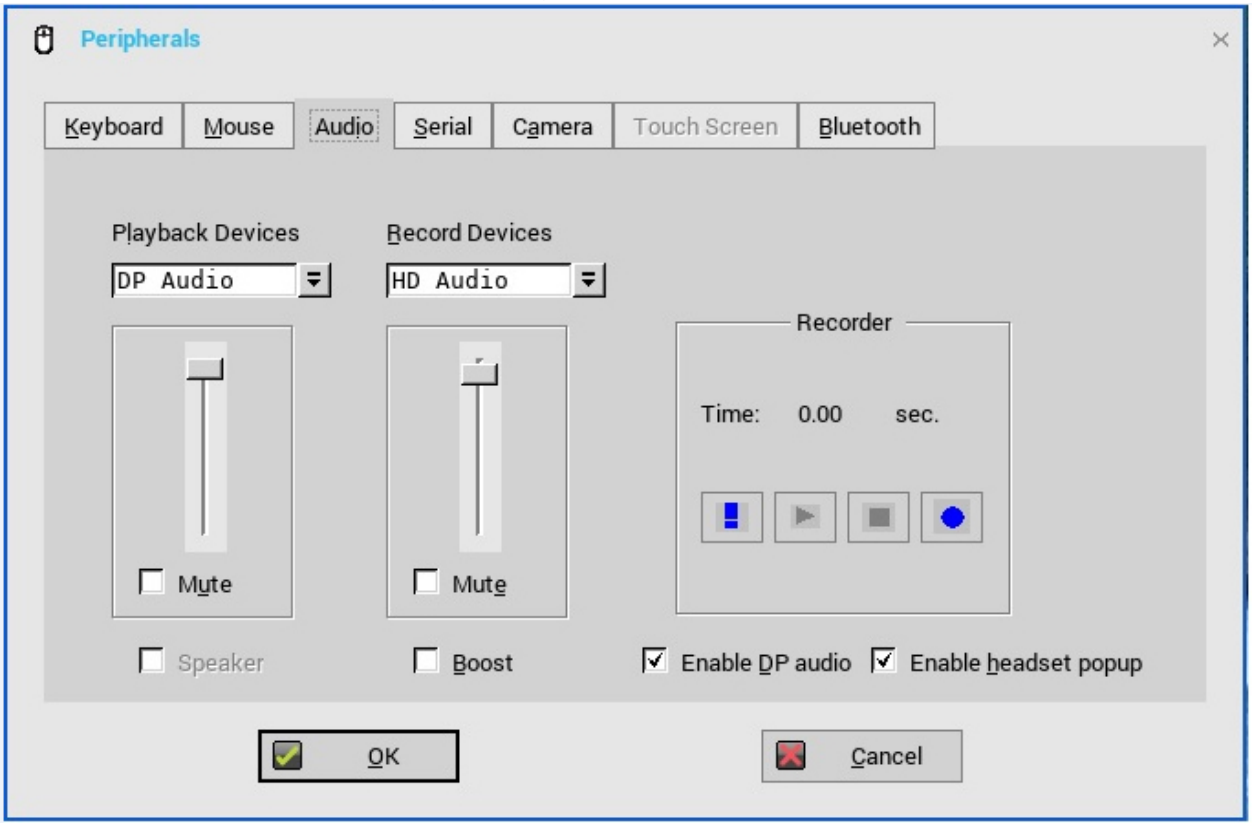

Figure 12. Audio

- Analog Headset Popup

  Select the **Enable headset popup** check box to display the headset popup dialog box when you connect an analog headset to the front audio 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. You can also use an INI parameter to enable or disable the headset popup dialog box. For more information about the INI parameter, see INI parameters.

For the list of known issues about the DisplayPort audio, see Known issues.

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 reader such as Dell KB-813.

Management suite support

Wyse 5070 thin client can be managed using Dell Wyse Management Suite version 1.2. For more information, see Dell Wyse Management Suite Administrator's Guide.

Simplified Certificate Enrollment Protocol enhancement

In this release, Simplified Certificate Enrollment Protocol (SCEP) supports both HTTP and HTTPs protocol for **RequestURL**. You can add the protocol prefix before the URL.

Other references

- **E-star**—ThinOS 8.5.1 passed E-star 6.1 and E-star 7.0 with DP1, the resolution for E-star 7.0 is in progress post RTS.
- **IPv6**—Certification is in progress post RTS.
- **DIMM**—2 x 4 GB DIMM RAM performance improvement is in progress post RTS.

Supported platforms

Table 1 describes the supported platforms and associated firmware in this release.

Table 32. Supported platforms

Platform	ThinOS	ThinOS with PCoIP
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

BIOS information

Table 2 describes the latest BIOS information in this release.

Table 33. BIOS information

Platform	BIOS version	BIOS BIN file name—for ThinOS update
Wyse 5070 thin client—Celeron	Dell BIOS 1.0.3	X10_bios.bin
Wyse 5070 thin client—Pentium	Dell BIOS 1.0.3	X10_bios.bin
Wyse 5070 Extended thin client	Dell BIOS 1.0.3	X10_bios.bin

Package details

Table 3 describes the package details in this release.

Table 34. Packages for 8.5_107 build

Package name	Version
FR.i386.pkg	1.20.46089
horizon.i386.pkg	4.6.47367
RTME.i386.pkg	2.3.44433

Package name	Version
TCX.i386.pkg	7.1.41853

Table 35. Packages for 8.5_108 build

Package name	Version
horizon.i386.pkg	4.6.47369
TCX.i386.pkg	7.1.41853
RTME.i386.pkg	2.3.44433
FR.i386.pkg	1.20.46089

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, do the following:

1. 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 file server—ftp or https.
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.

The 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*.

BIOS configuration on Wyse 5070 thin client

Table 11 describes the INI parameters to configure Dell BIOS settings on Wyse 5070 thin client.

Table 36. INI parameters

INI parameters	Description
Device=DellCmos [CurrentPassword=password] [CurrentPasswordEnc=password encrypted] [NewPassword=password] [NewPasswordEnc=password encrypted] [Audio={yes, no}] [AdminLock={yes, no}] [AutoPower={Disable, Daily, Workday, Days}] [AutoPowerTime=hh:mm] [AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}] [ACRecovery={PowerOff, PowerOn, LastState}] [USBRearPort={yes, no}] [USBFrontPort={yes, no}] [WakeOnLan={Disable, LAN, PXE}] [WakeOnUSB={yes,no}] [USBBootSupport={yes, no}] [PXEBootSupport={yes, no}]	These INI parameters are applicable to thin clients with Dell standard BIOS. Supported platforms: • Wyse 3040 thin client • Wyse 5070 thin client **[CurrentPassword=password]**—This option provides the current BIOS password for changing BIOS settings when device's admin password is available. **[CurrentPasswordEnc=password encrypted]**—This option is used to provide encrypted current password. **[NewPassword=password]**—This option is used to change device's password. Current Password is not required if device's admin password is not available. **[NewPasswordEnc=password encrypted]**—This option is used to provide encrypted new password. **NOTE: Password encrypted is of higher priority. For example: If both CurrentPassword and CurrentPasswordEnc are configured, then CurrentPasswordEnc overwrites the CurrentPassword.** **[Audio={yes, no}]**—This option enables or disables the integrated audio controller. BIOS default value is **yes**. All Dell BIOS settings take effect after the power off restart. **[AdminLock={yes, no}]**—When enabled, this option prevents user from entering setup when an admin password is set. Default value is **no**. **[AutoPower={Disable, Daily, Workday, Days}]**—This option sets the time of day when you want the system to automatically turn on. **No/Disable**—The system does not automatically power up; **Yes/Daily**—The system power ups every day at the time specified in AutoPowerTime; **Workday**—The system power ups Monday through Friday at the time specified in AutoPowerTime; **Days**—The system power ups on the days specified in AutoPowerDays. **[AutoPowerTime=hh:mm]**—This option specifies the auto power on time, value range of hh is 0–23, while mm is 0–59. **[AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]**—This option specifies the days to power up system automatically. For example, Device=DellCmos AutoPower=Days AutoPowerTime=2:30 AutoPowerDays=Sunday; Friday; Saturday

INI parameters	Description
	[ACRecovery={PowerOff, PowerOn, LastState}]—This option specifies how the system behaves when AC power is restored after an AC power outage. • PowerOff—System stays off after AC power is restored. • PowerOn—System powers on after AC power is restored. • LastState—System keeps the last power state as the last/ previous state of the system was before AC power was removed. **[USBRearPort={yes, no}]**—If yes is specified, devices attached to the rear USB port are enabled, and available for operating system. If no is specified, operating system cannot detect any devices attached to the back USB port. **NOTE: USB keyboard and mouse always work in the BIOS setup irrespective of this setting.** **[USBFrontPort={yes, no}]**—If yes is specified, devices attached to the front USB port are enabled and available for operating system. If no is specified, operating system cannot detect any device attached to front USB port. **NOTE: USB keyboard and mouse always work in the BIOS setup irrespective of this setting.** **[WakeOnLan={Disable, LAN, PXE}]**—This option allows the thin client to power up from the off state when triggered by special LAN signal. Wakeup from the standby state is unaffected by this setting and must be enabled in the operating system. This feature only works when the thin client is connected to AC power supply. • Disable—Do not allow the system to power on by special LAN signals when it receives a wake up signal from the LAN or wireless LAN. • LAN—Allows the thin client to be powered on by special LAN signals. • PXE—A wake up packet sent to the system in either the S4 or S5 state causes the system to wake up, and immediately boot to PXE. **[WakeOnUSB={yes, no}]**—WakeOnUSB allows the computer to power up from the off state when triggered by USB signal. Wakeup from the standby state is unaffected by this setting and must be enabled in the operating system. This feature only works when the computer is connected to AC. • If yes is specified, wake on USB is enabled. • If no is specified, wake on USB is disabled. **[USBBootSupport={yes, no}]**—If yes is specified, device allows operating system to boot from USB port. If no is specified, the operating system cannot boot device from USB port. **NOTE: USB, keyboard, and mouse always work regardless of being specified or not.** **[PXEBootSupport={yes, no}]**—If yes is specified, device allows operating system to boot from PXE. If no is specified, the operating system cannot boot device from PXE.

INI parameters

Table 37. INI parameters

<table>
<tr><th>INI parameters</th><th>Description</th></tr>
<tr><td>ConnectionBroker={default, VMware, Microsoft, Quest, AWS}

*[EnableUnauthenticatedAccess]={yes, no}</td><td>This option specifies the type of VDI broker.
For VMware broker, ConnectionBroker=VMware is recommended. ConnectionBroker=VDM is still supported but deprecated.

Set EnableUnauthenticateAccess=yes to enable VMware View broker login anonymously. The default value is no.</td></tr>
<tr><td>*ScreenSaver=value[LockTerminal={0, 1, 2, 3}]
[Type={0, 1, 2, 3, 4, None}]</td><td>
<table>
<tr><th>Value</th><th>Delay before starting</th></tr>
<tr><td>0</td><td>Disabled</td></tr>
<tr><td>1</td><td>1 minute</td></tr>
<tr><td>3</td><td>3 minutes</td></tr>
<tr><td>5</td><td>5 minutes</td></tr>
<tr><td>10</td><td>10 minutes</td></tr>
<tr><td>15</td><td>15 minutes</td></tr>
<tr><td>30</td><td>30 minutes</td></tr>
</table>
The default screen saver value is 10 minutes, and the maximum value is 180 minutes. The value can be from 0 to 180. If the value defined is not from the table, then the value is added to the drop-down list on the GUI.
The optional parameter Type specifies which type of screen saver to use. In case of Type=None and LockTerminal as non-zero, the unlocking window is displayed after the screen saver time is up.
<table>
<tr><th>Value</th><th>Type of screen saver</th></tr>
<tr><td>0</td><td>Blank the Screen</td></tr>
<tr><td>1</td><td>Flying Bubbles</td></tr>
<tr><td>2</td><td>Moving Image</td></tr>
<tr><td>3</td><td>Showing Pictures</td></tr>
<tr><td>4</td><td>Playing Video</td></tr>
<tr><td>None</td><td>None</td></tr>
</table>
</td></tr>
<tr><td>*SessionConfig=Blast

[EnableH264={yes, no}]

[NetworkCondition={Excellent, Typical, Poor}]</td><td>This INI parameter controls the Blast H264 feature and works only when the resolution is greater than 1920 where the H.264 is automatically disabled by default. The default value of this parameter is yes, which enables H264; if the value is set to no, then it disables H264.

NOTE: H.264 is enabled with resolution width less than or equal to 1920, and disabled with resolution width greater than 1920. You can use this INI parameter to enable H.264 when resolution width is greater than 1920. However, the performance is downgraded.

The option NetworkCondition controls the Blast network condition. The default value is Typical. The options are:</td></tr>
</table>

INI parameters	Description
	• Excellent—network is good • Typical—network is normal • Poor—network is bad The Blast Extreme connection selects either UDP or TCP based on the network conditions. When the network is excellent and typical, the Blast Extreme connection selects the TCP. When it is poor, the Blast Extreme connection selects UDP.
Service=vncd disable={yes, **no**} [servers=server_list] *[HttpPort=_http_port_] *[TcpPort=_tcp_port_]	**Service=vncd disable**—Yes/no option to disable the vncd service, same as MaxVncd={0, 1}. Default value is no. **servers**—Use the servers option to limit the valid vncd client site to the IP addresses in the server_list parameter, which contains IPv4 IP or IP range addresses, such as 192.168.1.0/24; 192.168.2.48. If this option is not set, then all IP addresses are displayed as valid. • service vncd—supports both http and tcp connections. • HttpPort—sets the http port for vncd service, the default port is 5800. • TcpPort—sets the tcp port for vncd service, the default port is 5900.
ResourceURL={yes, **no**} *[Type={Picture, Firmware, Package}]	The resource files have their specified default path in file server, for example, the pictures for Showing Picture screen saver are from the folder **/wnos/picture** in file server (default), and the bitmap are from **/wnos/bitmap**. **ResourceURL**—If this option is set to yes, the subsequent options are use to configure one or more resource URLs. The system fetches the resource files from the new URL. If this option is set to no, all the subsequent options are ignored. • Set Type=Picture to specify the url of pictures for **Showing Picture** screen saver. • Set Type=Firmware to specify the url for ThinOS image, BIOS image, hosts, printermap, and noticefile. • Set Type=Package to specify the url for packages. For example, ResourceUrl=yes \ type=picture url=**ftp://10.xxx.xxx.xx/pic1** user=pteng password=xxxxxx encrypt=no \ type=firmware url=**http://10.xxx.xxx.x/wnos1** user=administrator password=XXXXXX encrypt=yes \ type=package url=**https://10.xxx.xxx.xxx/wnos/pkg2** user=abc password=yyyy
DESKTOP=bitmap file [Layout={tile, center, **stretch**}] [IconTextColor="rrr ggg bbb"]	**Desktop**—Specifies the bitmap file to be used as wallpaper for the local desktop. This file could be a 4-bit, 8-bit, or 24-bit BMP file or a standard GIF file or a standard JPEG file. The file must be located in the FTP server **wnos\bitmap** directory. Default is **DELL wallpaper**. When bitmap file is set in **wnos.ini**, at next re-boot, the thin client will not show DELL default wallpaper until INI wallpaper is loaded. To recovery the DELL default wallpaper, set Desktop=DELLDEFAULT in **wnos.ini** or do factory reset. When you set Desktop=WYSEDEFAULT, the old DELL logo wallpaper is displayed before 8.5.0 build is loaded. When you set Desktop="", the wallpaper is disabled.
SignOn={**yes**, no, NTLM}	**SignOn**—Default is yes. Yes/no/NTLM option to enable the sign-on process. If set to NTLM, a user can be authenticated with an NTLM protocol.

INI parameters	Description
*[SCRemovalBehavior= {none or -1, **logoff or 0**, lock or 1, killsessions or 2}]	The user must be a domain user, and the same sign-on user credentials must be available in the **ftp://~/wnos/ini/**directory. Set SCRemovalBehavior=killsessions can be used along with the **AutoSignoff** parameter.
Device=vusb *[TCXDVCdefault={yes, **no**}]	The default value is no. Set **yes** for RDP to establish the first connection faster when USB device is redirected.
Privilege=None TCPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF] UDPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF]	**TCPTosDscp**: Use this option to set the TOS field of all TCP packets when the fields are not pre-configured by other INI settings. **UDPTosDscp**: Use this option to set the TOS field of all UDP packets when the fields are not pre-configured by other INI settings. Added new sheet TOS_Priority_settings for TosDSCP INI, which is merged from TOS_Priority_settings.docx. For more information, see TOS priority settings for TosDSCP INI.
SecurityPolicy={full, **warning**, low} *[TLSCheckCN=[**yes**, no]]	Specifies the global security mode for SSL connection. If application SecurityMode is default, application applies the setting. If set to full, the SSL connection must verify server certificate. If it is untrusted, connection is dropped. If set to warning, the SSL connection musts verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, and the default value is warning. For those SSL connections with their own security policy, this does not impact. For example, • File server with https protocol has its own security mode (Full, Warning and None), the default is Full. • VMware View and AWS broker have its own security mode (Full, Warning and None), the default is Warning. • Citrix broker, RDS broker, and SECUREMATRIX force to high security mode The option **TLSCheckCN** enables/disables the ThinOS client to check server certificate common name when connecting to SSL in full security mode. This option does not effect the SSL connections of VMware View, Amazon Workspaces, and VPN. These three connections checks server certificate common names all the time. The default value is changed to **yes** from build version 8.5_106. **NOTE: Use NetBIOS or FQDN values to define an SSL (Https) connection when enabling TLSCheckCN option (TLSCheckCN=yes), enabling TLSCheckCN results in SSL connection failure (SignOn failures) when an IP address is defined.**
*Device=mouse[Speed=[1-9]] [Swap={yes, **no**}] [FlipFlopWheel={yes, **no**}] [Big={yes, **no**}]	The Speed is used to configure mouse's moving speed. 1 is the slowest, 9 is the fastest. The default value is 6. This parameter is the replacement of **MouseSpeed**. If Swap=yes is set, right button is set as primary button. The default value is no. Set MouseFlipFlopWheel=yes to invert the mouse scroll wheel, the default value is no. If Big=yes is set, the size of local mouse pointer is increased by two times. The default value is no. This is designed for Wyse 5070 thin client only.
Dualhead=[yes, no] *[ManualOverride=[yes, no]] *[Taskbar=["wholescreen", "mainscreen"]]	Dualhead parameter is applicable for Wyse 5070 thin client. If ManualOverride=yes, all the parameters are only valid in factory default. It allows you to configure display setting manually if both single monitor and a dual monitor exist in an environment. This is not applicable for Wyse 5070 thin client.

INI parameters	Description
	Taskbar—Specifies the style to be used for taskbar. The option wholescreen places the taskbar at the bottom of the entire screen. The option mainscreen places the taskbar at the bottom of the main screen. This is not applicable for Wyse 5070 thin client.
Device=audio *[jack_popup=[**yes**, no]	Specifies the ThinOS local audio setting. The default value of jack_popup option is **yes**. If jack_popup=no, it disables jack popup selection message when headset jack is plugged in.
ScepAutoEnroll={yes, no} AutoRenew={yes, no} InstallCACert={yes, no} [CountryName=country] [State=state] [Locality=locality] [Organization=organization_name] [OrganizationUnit=organization_unit] [CommonName=common_name] [Email=email_address] KeyUsage=key_usage KeyLength={1024, 2048, 4096 } [subAltName=subject_alt_name_list] RequestURL=scep_request_url CACertHashType={MD5, SHA1} CACertHash=CA_HASH_VALUE [EnrollPwd=enrollment_password] [EnrollPwdEnc=encrypted_enrollment_password] [ScepAdminUrl=scep_administrator_page_url] [ScepUser=scep_enrollment_user]	This option is to allow client automatically get certificates and renew certificates using SCEP protocol. **ScepAutoEnroll**—Set this keyword to yes to enable client's functionality to automatically obtain certificate. Set **AutoRenew**—Set this keyword to yes to enable certificate auto renew. Client only tries to renew certificates requested either manually or automatically through SCEP from this client, and the renewal is performed only after a certificate's 1/2 valid period has passed. Set **InstallCACert**—Set this keyword to yes to install the root CA's certificate as trusted certificate after successfully getting a client certificate. **CountryName**, **State**, **Locality**, **Organization**, **OrganizationUnit**, **CommonName**, **Email**—These keywords together compose the subject identity of the requested client certificate. Country Name should be two letters in uppercase, other fields are printable strings with a length shorter than 64 bytes, and email_address should have a '@' in it. At least one of the preceding fields must be configured correctly to form the client certificate's subject identity. **KeyUsage**—This option is to specify key usage of the client certificate and should be set to a digitalSignature, keyEncipherment or both using a ';' concatenating these two as digitalSignature; keyEncipherment. **KeyLength**—This option is used to specify the key length of the client certificate in bits, must have one of the values in the list. **subAltName**—This option is to specify the client certificate's subject alternative names. It is a sequenced list of name elements, and every element is either a DNS name or an IP address. Use ';' as delimiter between them. *__RequestURL__—This option is to specify the SCEP server's service URL. This field must be set correctly. The default protocol for SCEP service is HTTP, and data security is ensured by SCEP itself. You can also add **https://** prefix if SCEP service is deployed on HTTPS in your environment. *__CACertHashType__—This hash type is used to verify certificate authority's certificate, should be set to MD5 or SHA1 or SHA256. **CACertHash**—This is the hash value used to verify certificate authority's certificate. Client does not issue a certificate request to a SCEP server and cannot pass certificate chain checking through a valid certificate authority. **EnrollPwd** or **EnrollPwdEnc**—These keywords are used to set the enrollment password from a SCEP administrator. **EnrollPwd** is the plain-text enrollment password and **EnrollPwdEnc** is the encrypted form of the same enrollment password. Use only one of these two fields to set the used enrollment password. As a substitute of using EnrollPwd or EnrollPwdEnc to directly specify an enrollment password, client allows using a SCEP administrator's credential to automatically get an enrollment password from a Windows SCEP server. In this case, the **ScepUser**, **ScepUserDomain**, **ScepUserPwd** (or ScepUserPwdEnc, in encrypted form instead of

INI parameters	Description
	plan-text) are used to specify the SCEP administrator's credential, and ScepAdminUrl must be set correctly to specify the corresponding SCEP admin web page's URL. If EnrollPwd or EnrollPwdEnc is set, client tries to use these set of settings to automatically get an enrollment password and then use that password to request a certificate. If communication security is necessary in your environment during this phase, add **https://** as the prefix for ScepAdminUrl to use HTTPS instead of the default HTTP protocol. Use ScepAutoEnroll=no AutoRenew=yes to only enable SCEP auto renew; all other parameters are not needed if ScepAutoEnroll is set to no.
SessionConfig=RDP *[GracefulReconnTimeout={10 - 100}]	You can set SessionConfig=RDP to establish the default setting for RDP sessions. The option enables you to set a timeout for RDP to reconnect the session. If there is no response from the server during this time period, it avoids the RDP session to stop responding for a long time and cannot auto-reconnect due to poor network connection or short time network disconnection. There is no default value for this option; the feature is disabled if it is not set. The valid value is 10 to 100, in seconds.
SessionConfig=PCoIP *[DisableRTAV=[yes, **no**]]	**SessionConfig**— Specifies the PCoIP default settings of the optional connection parameters for all PCoIP sessions. The option DisableRTAV can disable the RTAV virtual channel in a session for RTAV virtual channel which may impact the performance of some audio or video related applications. The default value is no.
PnliteServer=List of {IP address, DNS names or URLs} *[IgnoreDefaultGateway=[yes, no]]	A list of host names or IP addresses with optional TCP port number or URLs of PN-Lite servers. The default value is empty. Each entry with an optional port is specified in the format `Name-or-IP:port`, where `:port` is optional. If port number is not specified, port number 80 is used. When you specify a port number, it is saved in the non-volatile memory. The IgnoreDefaultGateway option ignores the default gateway of the current selected store during Netscaler login. You must always use pnliteserver to continue. The value yes is used to ignore. The default value is no that uses default gateway as the Netscaler server to reset login again.
IEEE8021X=[yes, no] *[network={wired, wireless}] *[wiredreset=[yes, no]]	If IEEE8021X is set to no, then all other parameters following the parent parameter are ignored. Also, network is not configured, and the configuration is ignored. The option wiredreset is used to reset the MII when **authenticate cancel** occurs. This option is only for wired network, and it is disabled by default.
SessionConfig=ICA *[DisableMMRSeek =[yes, no]]	You can set ICA to establish the default settings for ICA sessions. The DisableMMRSeek option can be used to disable the MMR seek capability on the client side. The default value is no. It might cause trap while enabling this setting with some specific servers, for example, Windows 10 IoT Enterprise.
AdminMode=[yes, no] *[ShowAESButton=[yes, no]]	AdminMode—Default is no. Yes/no option to use the username and the password to obtain a high thin client configuration when the privilege parameter level is set to high (Privilege=high). If ShowAESButton=yes is specified, and you enter into the admin mode, the AES Encrypt button is displayed in the `System Admin` dialog box. Press this button to launch the encrypted generator to generate enc-password for INI settings. You can set ShowAESButton=no to hide this button. If Enc-Username and Enc-Password are available, then the default value is yes, or the default value is no.

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

TOS priority settings for TosDSCP INI

Routers treat network packets differently based on priority of the TOS tag in the IP header.

IP header has a 1-byte field called TOS—Type of Service.

IP precedence is older than DSCP. DSCP is compatible with IP Precedence.

Table 38. TOS priority settings

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
IP precedence	IP precedence							
DSCP	DSCP							
	Class Selector			Drop Precedence				

CS1 Dscp (001 000) match packets with precedence 1 (Low)

CS2 Dscp (010 000) match packets with precedence 2

CS3 Dscp (011 000) match packets with precedence 3

CS4 Dscp (100 000) match packets with precedence 4

CS5 Dscp (101 000) match packets with precedence 5

CS6 Dscp (110 000) match packets with precedence 6

CS7 Dscp (111 000) match packets with precedence 7 (High)

Table 39. TOS priority settings

IP precedence (3 bits)			DSCP (6 bits)				
Name	Value	bits	Per-Hop behavior	ClassSelector	DropPrecedence	Code point Name	DSCP Bits(decimal)
Routine	0	0	Default	NA	NA	Default	000 000 (0)
Priority	1	1	AF	1	1.Low	AF11	001 010 (10)
					2.Medium	AF12	001 100 (12)
					3.High	AF13	001 110 (14)
Immediate	2	10	AF	2	1.Low	AF21	010 010 (18)
					2.Medium	AF22	010 100 (20)
					3.High	AF23	010 110 (22)
Flash	3	11	AF	3	1.Low	AF31	011 010 (26)

IP precedence (3 bits)			DSCP (6 bits)				
					2.Medium	AF32	011 100 (28)
					3.High	AF33	011 110 (30)
Flash Override	4	100	AF	4	1.Low	AF41	100 010 (34)
					2.Medium	AF42	100 100 (36)
					3.High	AF43	100 110 (38)
Critical	5	101	EF	NA	NA	EF	101 110 (46)
Internetwork Control	6	110	NA	NA	NA	NA	(48-55)
Network Control	7	111	NA	NA	NA	NA	(56-63)

Table 40. TOS priority settings

IP precedence (3 bits)		DSCP (6 bits)	
Name	**Useful**	**Name**	**Useful**
Routine	Try as usual	NA	NA
Priority	For data traffic	AF11	Big block data
Immediate		NA	NA
Flash	For Voice control data	NA	NA
Flash Override	Video streaming	NA	NA
Critical	Voice Data	EF	Interactive Voice
Internetwork Control	Reserved	NA	NA
NetworkControl		NA	NA
		NA	NA

NOTE: The information in this section is leveraged based on the research on web. Specific priority designs must be arranged by network architect.

Tested environment

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

Table 41. Tested environment

Component	Version
WMS	1.2
WDM	5.7.2
Imprivata OneSign	5.3.001.11
Caradigm	6.3.1
NetScaler	10.1/11.0/11.1/12.0
Store Front	2.6/3.6/3.12
Web Interface	5.4
SecureMatrix	4.1.0

Table 42. Tested environment

	Windows 7	Windows 8.1	Windows 10	Linux	Windows 2008 R2	Windows 2012 R2	Windows 2016	APPs
VMware Horizon 7.3	√	√	√	√	√	√	√	√
XenDesktop 5.6	√							
XenApp 6.5					√			√
XenDesktop/ XenApp 7.6	√	√			√	√		√
XenDesktop/ XenApp 7.15 LTSR CU1	√	√	√		√	√	√	√
Tera PCM for AWS 1.03	√ *							
RDP/RDS 2012 R2/RDS 2016	√	√	√		√	√	√	√

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

Table 43. Tested environment

XenDesktop/ XenApp	Operating System	RTME	Lync client	Lync server	Skype for Business (SFB) server
7.6	Windows 8.1	1.8	Lync 2013	Lync 2013	
	Windows 2012 R2	2.3	Skype For Business 2015		Skype For Business 2015
7.15	Windows 7	2.3	Skype For Business 2016		Skype For Business 2015
	Windows 8.1	2.3	Skype For Business2016		Skype For Business 2015
	Windows 10	2.3	Skype For Business 2016		Skype For Business 2015

XenDesktop/ XenApp	Operating System	RTME	Lync client	Lync server	Skype for Business (SFB) server
	Windows 2016	2.3	Skype For Business 2016		Skype For Business 2015

Peripherals list

This section lists the supported peripheral devices and peripheral ecosystem.

- **Keyboard/ Mouse**
  - Dell USB Wired Keyboard - KB216
  - Dell USB Wired Laser Mouse - Naruto
  - Dell USB Wired Optical Mouse - MS116
  - Japanese Keyboard - KB216
  - Dell KM636 Wireless Keyboard and Mouse
  - DELL wireless Keyboard/mouse KM632
  - DELL wireless Keyboard/mouse KM714
  - Dell Keyboard KB113p
  - Dell Keyboard KB212-B
  - Dell Keyboard KB216p
  - Dell keyboard KB813—Smart card reader
  - Dell Mouse MS111-P
  - Dell Mouse MS116-P
  - Dell Keyboard SK-3205—Smart card reader
  - Dell Optical Wireless Mouse – WM123
  - Dell Wireless Mouse – WM324
  - Logitech K480 Keyboard, Bluetooth
  - Logitech K400 Plus
  - Logitech M557 mouse, Bluetooth
  - Microsoft Arc Touch Mouse 1428
  - Microsoft ARC touch mouse 1592, Bluetooth
  - Thinkpad Compact Bluetooth Keyboard—Bluetooth
  - Rapoo E6100, Bluetooth
  - Cherry RS 6700 USB—Smart card reader
  - SpaceNavigator 3D Space Mouse
- **USB Webcam**
  - Logitech C270 HD Webcam
  - Logitech C525 HD Webcam
  - Logitech C920 HD Pro Webcam

    NOTE: Skype for Business 2015 is not supported.
  - Logitech C930e HD Webcam—Logitech Carl Zeiss Tessar HD 1080p Webcam
  - Logitech BCC950 ConferenceCam
  - Logitech USB Webcam 9000
  - Microsoft LifeCam 3.0 Cinema—Microsoft LifeCam 3.0 Cinema P/N X821404-001
  - Microsoft LifeCam HD-3000
  - Microsoft LifeCam Studio
- **Printer**
  - Dell B1163 Mono Multifunction printer

NOTE:
- Local test print is not supported.
- Mapping is supported through Citrix UPD with PCL 5 class.
- Redirection is supported.

– Dell B1165nfw Mono Multifunction printer

NOTE:
- Local test print is not supported.
- Mapping is supported through Citrix UPD with PCL 5 class.
- Redirection is supported.

– Dell B1260dn laser printer
– Dell B1265dnf Multifunction laser printer

NOTE: Citrix UPD supports only PCL 5 and PCL 4 class

– Dell B2360d laser printer
– Dell B2360dn laser printer
– Dell B2375dnf Mono Laser Multifunction printer
– HP LaserJet P2055d
– HP LaserJet P2035
– HP LaserJet 1022n
– HP Color LaserJet CM1312MFP
– EPSON PLQ-20K—Impact printer

- **Mobile device**
  – Samsung Galaxy S7
  – iPhone7—iOS11.2.6
  – HTC one-XL—Android 4.2.2
- **USB headset**
  – Dell Pro Stereo Headset - Skype for Business - UC350
  – Professional Sound Bar - Skype for Business - AE515
  – Dell USB Sound Bar - AC511
  – Jabra Pro 935 MS Wireless headset, Mono - Office Centric
  – Jabra PRO 935 MS
  – Jabra Speak 510 MS, Bluetooth—Bluetooth
  – Jabra BIZ 2300 Duo, USB, MS
  – Jabra BIZ 2400 Duo USB MS
  – Jabra UC SUPREME MS /LINK 360, Bluetooth
  – Jabra UC Voice 550 MS Duo
  – Jabra UC Voice 750MS Duo Drk
  – Jabra GN2000
  – Plantronics BLACKWIRE C420
  – Plantronics BLACKWIRE C520
  – Plantronics BLACKWIRE C710, Bluetooth

NOTE: Tested with USB connectivity.

  – Plantronics SAVI W740 3IN1 Convertible, UC, DECT 6.0 NA, Bluetooth
  – Plantronics SAVI List 400 series
  – Plantronics Voyager Legend UC B235 NA, Bluetooth—Bluetooth
  – Plantronics Calisto P240 D1K3 USB handset
  – Plantronics Calisto 620-M, Bluetooth
  – Plantronics DA60

- Plantronics P420
- Plantronics USB DSP DA40(B)
- SENNHEISER USB SC230
- SENNHEISER SC 660 Binaural CC&O HS, ED
- SENNHEISER SC 260 USB MS II
- SENNHEISER SP 10 ML Speakerphone for Lync
- SENNHEISER SC 660 USB ML
- SENNHEISER D 10 USB ML-US Wireless DECT headset
- SENNHEISER SC 260 USB MS II
- SENNHEISER SC 75 USB MS
- POLYCOM Deskphone CX300
- Jabra PRO 9470, Bluetooth

  NOTE: Bluetooth standard is not supported.

- **Analog headset**
  - Logitech h150—CTIA standard
  - Philips—CTIA standard
  - LFH3200/00 SPEECHMIKE PREMIUM

    NOTE: Need force redirect to use all the features, set INI Device=vusb ForceRedirect=VID,PID,0x00,0x00,0x00.
  - Dell USB SoundBar AC511

    NOTE: Blast session is not supported.
- **Monitor**
  - Dell 24 Monitor - E2417H
  - Dell 23 Monitor - E2318H
  - Dell 22 Monitor - E2218HN
  - Dell 20 Monitor - E2016H
  - Dell 19 Monitor - E1916H
  - Dell 24 Monitor - P2418HT—touch
  - Dell 24 Monitor - P2418HT—multi-touch (only in RDP session)
  - Dell 24 Monitor - P2417H
  - Dell 23 Monitor - P2317H
  - Dell 22 Monitor - P2217H
  - Dell 22 Monitor - P2217
  - Dell 20 Monitor - P2016
  - Dell 24 Monitor - U2415
  - Dell 43 Monitor - P4317Q
  - Dell 24 Monitor - MR2416
  - Dell 24 Monitor - P2415Q 4K2K (UHD) monitor
  - Dell UltraSharp 34 Monitor - P3418HW
  - Dell UltraSharp 27 Monitor - U2518D
  - Dell UltraSharp 27 Monitor - U2718Q—4K
  - Dell E2416Hb—1920x1080
  - Dell E2715Hf—1920x1080
  - Dell P2415Q—3480x2160
  - Dell P2714Hc—1920x1080
  - Dell P2715Q—3840x2160
  - Dell P2815Qf—3840x2160
  - Dell U2414HB—1920x1080
  - Dell U2415—1920x1200

- Dell U2713Hb—2560x1440
- Dell U2713HM—2560x1440
- Dell U2713HMt—2560x1440
- Dell U3415W—3440x1440
- Dell U2718Qb—3840x2160
- Dell U2718Q—3480X2160
- Dell U2913 WM—2560x1080
- Dell U3014t—2560x1600
- Dell S2718D—2560x1440
- Dell S2817Q—3840x2160
- Dell D2215Hc—1920x1080
- Dell UZ2315H—1920x1080
- Dell 3008WFP—2560x1600

- **DVD ROM**
  - BENQ DVD Drive
  - Samsung portable DVD Writer SE-208
  - Dell external DVDRW Drive
  - Dell DW316
- **Cable/Converter**
  - DisplayPort to HDMI adapter
  - DisplayPort to VGA adapter
  - USB Type-C to DisplayPort adapter
  - USB Type-C to HDMI
  - USB Type-C to VGA adapter
  - USB to Serial adapter - Trendnet
  - USB to Serial adapter - Cables-2-Go
  - Dell miniDP-VGA convertor
  - Dell TYPE-C-VGA convertor
  - Dell DP-VGA convertor
  - Dell DP-DVI convertor
  - Dell TYPE-C-DP convertor
  - Dell TYPE-C-HDMI convertor
  - Dell KDP70 Adapter converts DisplayPort to DVI—Dual-Link
  - TRANSITION SGFEB 1040-120—Fiber convertor
  - USB to Serial converter
  - USB-C to USB 3.0
  - USB-C Male to USB-A Female adapter cable
- **Smart card reader**
  - OMNIKEY HID 3021
  - OMNIKEY OK CardMan3121
  - SmartOS powered SCR335
  - Cherry keyboard RS 6600 with smart card
  - Cherry keyboard RS 6700 with smart card
  - Dell keyboard KB813—smart card reader
  - Dell Keyboard SK-3205—smart card reader
  - Gemalto IDBridge CT710
  - HID OMNIKEY 3121
  - HID OMNIKEY 5321
  - HID OMNIKEY 5422

- Dell Keyboard KB-813
- Cherry Keyboard KC-1000
- SCR 3310
- Wyse 5070 thin client - Onboard smart card reader

- **Smart card**
  - G&D FIPS 201 SCE 3.2
  - Gemalto TOPDLGX4 144
  - SafeNet SC650
  - Oberthur ID One 128 v5.5
- **Proximity Card Reader**
  - RDR-80581AKU
  - RDR-80582AKU
  - RDR-6082AKU
  - OMNIKEY 5025 CL
  - OMNIKEY 5326 DFR
  - OMNIKEY 5427 CK
- **Proximity/smart card reader**
  - OMNIKEY 5125
  - OMNIKEY 5325 CL
- **Finger Print Reader**
  - Finger Print Keyboard KSI 1700—Key Source International (KSI)
  - Finger Print Reader ET710—Upek
- **Touch screen**
  - Elo Touch Screen USB
  - Elo Touch Screen Serial
  - Dell P2418HT—1920x1080

    NOTE: Multi touch is supported only for RDP and not supported for ICA session and on the local system.
- **USB drive**
  - SanDisk USB 3.0 16 GB
  - SanDisk cruzer 16 GB
  - Sandisk cruzer 8 GB
  - SanDisk USB3.1 and Type-C 16 GB
  - Kingston DataTraveler 100 G3
  - Kingston DataTraveler G3 16 GB
  - Kingston DataTraveler G3 8 GB
  - Kingston DataTraveler Elite 3.0 16 GB
  - Kingston DTM30 32 GB
  - ADATA S107/16 GB
  - ADATA S102/16 GB
  - PNY USB3.0 16 GB
- **Networking**
  - Add On 1000 Base-T SFP transceiver (RJ-45) - 310-7225-AO
  - Allied Telesis 1 Gbps SFP transceiver - fiber connector - AT-SPSX-90
  - Allied Telesis 100 Mbps SFP fiber transceiver AT-SPFX/2-90
  - Allied Telesis 10/100/1000 RJ-45 SFP transceiver - copper (NOT TAA) - AT-SPTX
  - Dell Finisar 1 GB SFP - FTLF8519P3BNL
  - Dell Finisar 100 Mbps SFP - FTLF1217P2BTL-FC

Table 44. Smart card information from ThinOS event log

Smart Card info from ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 6.2	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1 (IDClassic 230)	ActivClient 6.2	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity V2	ActivClient 6.2	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
Gemalto/IDPrime.NET (Gemalto .net V2+)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	Axalto Cryptoflex.NET
Gemalto/IDPrime.NET (Gemalto .net 510)	Gemalto Mini driver 1.21X	Microsoft Base Smart Card Crypto Provider	Axalto Cryptoflex.NET(V7.2.1.0)
ID Prime MD v 4.0.2 (Gemalto 840)	Gemalto Mini driver 1.21X	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.3.2.11)
ID Prime MD v 4.1.0 (Gemalto 3810)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.4.0.7)
ID Prime MD v 4.1.1 (Gemalto 830)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.4.1.7)
ID Prime MD v 4.3.5 (Gemalto 830)	Gemalto Mini driver 1.21	Microsoft Base Smart Card Crypto Provider	IDPrime MD T=0 (V 7.6.5.4)
Etoken CardOS	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	Siemens CardOS V4.2B
Etoken CardOS (white USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	Siemens CardOS V4.2
Etoken Java(aladdin)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	eToken PRO Java SC 72K OS755
Etoken Java(aladdin) (blue USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	eToken PRO Java 72K OS755
Etoken Java(aladdin) (black USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java(aladdin) (black USB key)	SafeNet Authentication Client 8.2.133	eToken Base Cryptographic Provider	SafeNet eToken 5110
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	G&D STARCOS 3.0 T=0/1 0V300
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2
PIV (Yubico) (black USB key)	YubiKey PIV Manager	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_6.1.6	cv act sc/interface CSP	G&D STARCOS 3.2
ActivIdentity V2	ActiveClient 7.0	ActivClient Cryptographic Service Provider	Oberthur ID One 128 v5.5
ActivIdentity V2	ActiveClient 7.0	ActivClient Cryptographic Service Provider	G&D FIPS 201 SCE 3.2
ActivIdentity V2	ActiveClient 7.0	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4 144

Smart Card info from ThinOS event log	Driver	Provider (CSP)	Card type
SafeNet High Assurance Applets	SHAC v2.12.020	SafeNet Smart Card Key Storage Provider	SafeNet SC650 v4.1

Known issues

This section describes the known issues in this release.

Table 45. Known issues

Issue number	Issues description	Workaround
TL-923, BITS364686	A black or flickering screen is observed when you connect a 4K monitor to DP1 port on Wyse 5070 thin client with Intel Dual Band Wireless AC 9560 chipset. This issue is applicable to 8.5_107 build.	Configure the display resolution to less than 4K resolution on monitor connected to DP1 port. This is specific to DP1 port and independent of the devices connected to other ports.
TIR94834	After reboot, you cannot reconnect the Bluetooth headsets, and you must reboot headsets to reconnect. This functionality works as designed by Intel. This issue is applicable to 8.5_107 and 8.5_108 build.	Reopen the Bluetooth headset to reconnect.
TIR95564	After restoring the thin client to factory default settings, the Bluetooth connection may fail when you connect to a Bluetooth device the first time. However, the thin client connects to the Bluetooth device from second instance onwards. This issue is applicable to 8.5_107 and 8.5_108 build.	There is no workaround.
TIR96240	When you initialize the bluetooth, the screen flickers black only once before you disconnect the client from its power source and then turning on the client again (power cycling). This issue is applicable to 8.5_108 build.	This issue will be fixed in next release.
TIR95172	If you enable IPv6 for both ENET0 and ENET1, IPv6 routes through the Ethernet connection that fetches the IPv6 address first.	There is no workaround.
TIR95414	Hot plugging a monitor may result in a black screen in the VDI connected session. You must recover monitor to recover the session screen. The issue will be resolved in the next release.	Power off and power on the monitor, or remove the video cable from the client and connect the video cable to the port again.
TIR95681	Hot plugging a monitor during VDI connection or Display setup configuration may result in unexpected issues, such as terminal freeze or display layout change.	The issue will be resolved in the next release.
TIR95083	In Mirror mode with active session, 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.	You must manually reconnect the session after the resolution is changed.

Issue number	Issues description	Workaround
TL-645	DP audio on Wyse 5070 thin client works only with DP1/2 ports from Intel GPU using DP direct cable. It does not work with DP3 Intel GPU or AMD GPU mDP/DP ports. Also, it does not work with DP convertor cable.	There is no workaround.
TIR96028	Connect monitor to DP1 or DP2; either of the ports works correctly. For multimonitors, connect DP1 first, and then connect DP2, the DP audio works with DP1.	There is no workaround.
TL-745	DP audio option is not displayed on playback devices checklist if you insert DP cable in DP3 port or AMDDP or if you use any converter.	Reboot the thin client.
TIR95778	When you connect the monitor to DP1 and you upgrade the ThinOS firmware, the DP audio option may not be displayed in the **Peripherals** dialog box.	You must shut down and then power on the thin client.
TIR96293	SessionConfig=RDP, GracefulReconnTimeout=xx If you connect to RDP Windows 10 without RemoteFX session and enable H.264-AVC444, this ini parameter causes the session to autodisconnect and reconnect frequently. The thin client decoder may fail after several autoreconnect. After thin client decoder fails and after the main screen goes to sleep or you turn off the main screen, the session tries to show on the second screen automatically, and trap **winmgr** is observed. This issue is applicable to 8.5_108 build.	Disable, or do not configure the H.264-AVC444. If your network connection is good, then you need not set this ini parameter.
TIR94747, TIR95579, TIR95441, TIR95360, TIR95369, TIR95352, TIR95161	Occasionally launching a remote session using the VMWare Horizon BLAST protocol may result in the session not working.	Reconnect the session again.
TIR95561	When multiple high resolution monitors are used and set to **Span** mode, the display may get blurred.	Reduce the number of monitors that are set to **Span** mode.
TIR95098	When DHCP is not present, the **Out of Box Experience** may not work.	Press Ctrl+Esc to exit the **Out of Box Experience**.
TIR95648	Currently, multi-touch is not supported within Citrix Receiver sessions.	Use a Remote Desktop session.
TIR95336, TIR95353, TIR95414	When you connect a monitor with an active RemoteAPP session, the active RemoteAPP may not rescale, or the session screen may become blank.	Start the session again.
TIR95276	A black screen is observed, when you use a monitor connected to an integrated video, and modify the device's preference, and resetting the device to the factory default.	Reboot the thin client.
TIR95529	In some instances, a Citrix Receiver session may display a blurred screen.	Reconnect the session.
TIR95731	In some instances, a session may not be displayed when you connect VMware Horizon using the BLAST protocol.	Start the session again.
TIR95904	Display fall back may be observed on high resolution monitors.	This issue will be fixed in the future release.

Issue number	Issues description	Workaround
TIR95994	When you reconnect the displays, the application text may be scattered.	Reopen the window.

ThinOS 8.5_020 and ThinOS Lite 2.5_020

Priority and recommendations

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

Feature updates

This section contains information about the feature updates.

- VMware Horizon package is updated to version 4.6.50691 to support hardware cursor for Blast protocol.
- BIOS file names are updated for Wyse 5010 thin client, Wyse 5040 thin client, and Wyse 7010 thin client.
- Bloomberg keyboard in BIOS 1.0H is supported for Wyse 5060 thin client.
- OMNIKEY 5022 CL smart card reader is supported.
- Headless booting is supported.
- When there is an issue with the network during an active session with **Session Reliability** enabled, a warning message is displayed at the bottom-right of the screen.
- When there is a change to the WMS policy, a window is displayed with options **Restart Now** to apply the changes, and **Postpone** to delay the changes.

NOTE:

- For more information about the ThinOS features, see the *Dell Wyse ThinOS Version 8.5 Hotfix Administrator's Guide* at Dell.com/support.
- For more information about the newly added parameters, see the latest *Dell Wyse ThinOS Version 8.5 Hotfix INI Reference Guide* at Dell.com/support.

Supported platforms

The following table provides the list of supported hardware platforms.

Table 46. Supported platforms

Platform	Image filename	BIOS filename
Wyse 3010 thin client with ThinOS	DOVE_boot	Not available
Wyse 3010 zero client for Citrix	T00_xen.bin	Not available
Wyse 3020 thin client with ThinOS—T10D	T10D_wnos	Not available
Wyse 3020 zero client for Citrix	T00D_xen	Not available
Wyse 3030 LT thin client with ThinOS	U10_wnos	U10_bios.bin
Wyse 3030 LT thin client with PCoIP	PU10_wnos	PU10_bios.bin
Wyse 3040 thin client with ThinOS	A10Q_wnos	A10Q_bios.bin
Wyse 3040 thin client with PCoIP	PA10Q_wnos	A10Q_bios.bin

Platform	Image filename	BIOS filename
Wyse 5010 thin client with ThinOS—D10D	ZD10_wnos	D10G_bios.bin
Wyse 5010 thin client with PCoIP—D10DP	PD10_wnos	PD10G_bios.bin
Wyse 5010 zero client for Citrix	ZD00_xen	ZD00_bios.bin
Wyse 5040 AIO thin client—5212	ZD10_wnos	AIO10G_bios.bin
Wyse 5040 AIO thin client with PCoIP—5213	PD10_wnos	PAIO10G_bios.bin
Wyse 5060 thin client with ThinOS	D10Q_wnos	D10Q_bios.bin
Wyse 5060 thin client with PCoIP	PD10Q_wnos	PD10Q_bios.bin
Wyse 7010 thin client with ThinOS—Z10D	ZD10_wnos	Z10G_bios.bin

Packages

The following table provides the list of the packages that are available.

Table 47. Packages

Package name	Version
FR	1.20.46089
Horizon	4.6.50691
RTME	2.4.48792
TCX	7.1.41853

Tested environment

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

Table 48. Test environment

Product	Version
Wyse Management Suite	1.3.0
Wyse Device Manager	5.7.3
Imprivata OneSign	5.5
Caradigm	6.3.1
NetScaler	11.1/12.0
StoreFront	3.12
Web Interface	5.4
SecureMatrix	4.1.0

Table 49. Test environment

	Windows 7	Windows 8.1	Windows 10	Linux	Windows 2008 R2	Windows 2012 R2	Windows 2016	Apps
VMware Horizon 7.0	√	√	√	√	√	√	√	√
Citrix Virtual Apps and Desktops 5.6	√							
Citrix Virtual Apps 6.5					√			√
Citrix Virtual Apps and Desktops/ Citrix Virtual Apps 7.15	√	√	√		√	√	√	√
Tera PCM for AWS 1.03	√ *							
RDS 2012 R2/RDS 2016	√	√	√			√	√	√

*Amazon Workspace VM operating system—Windows 7 style—is actually based on 2008 R2 RDSH.

Table 50. Test environment

Citrix Virtual Apps and Desktops/ Citrix Virtual Apps	Operating system	RTME	Lync client	Skype for Business (SFB) server
7.15	Windows 7	2.4	Skype For Business 2016	Skype For Business 2015
	Windows 10	2.4	Skype For Business 2016	Skype For Business 2015
	Windows 2016	2.4	Skype For Business 2016	Skype For Business 2015

Fixed issues

The following table provides the list of fixed issues in this release:

Table 51. Fixed issues

Issue number	Description
TIR93953	Improved ThinOS PCoIP session reliability to prevent possible session disconnects when using Skype for Business and similar applications.
TIR96860	Client reboot warning message is displayed as a user notification for a pending reboot event through Wyse Management Suite.
TIR95720	The delay in publishing available desktops and applications to the ThinOS desktop is reduced, when Citrix Storefront URL with **Reconnect at logon** option is used.

Issue number	Description
TIR95744	In the Wyse 5060 thin client device, the BIOS is upgraded to address the issue where the client does not boot when a Bloomberg keyboard device is connected.
TIR95896/ TIR96347	Improved reliability to prevent USB device probe failures during boot or when connecting USB devices after boot.
TIR96019	Citrix session issue with error message **Session VDMMN aborted** is resolved.
TIR96091/TIR96211	The Wyse Management Suite ThinOS package deployment issues where ThinOS restarts before completing all package installations is resolved.
TIR96699	An issue where extended mouse buttons do not function with Blast protocol is resolved.
TIR95982	Olympus Dictation device reliability to prevent USB device probe failures at boot and while connecting the USB device after boot is improved.
TIR96577	Resolved a Citrix Virtual Apps and Desktops SSO issue when using the ID Prime MD smartcard 4.3.5 with Gemalto IDGo 800 middleware and a Gemalto IDBridge CT30 reader.
TIR96377	New ThinOS parameter to disable the print screen and system request keys. Device=Keyboard DisabledKeys=PrtScn;SysRq
TIR96378	Resolved a Blast protocol compatibility issue with Japanese 109 key keyboards.
TIR96545	Resolved a USB XHCI reset issue affecting Canon image FORMULA DR-C225 devices when redirected to Citrix Virtual Apps/Virtual Apps and Desktops.
TIR96432	Resolved an issue preventing the use of Swivel multifactor authentication with VMware Horizon.
TIR96651	Resolved an issue that resulted in slow display of updates at the beginning of the session when using Citrix published desktops with the PNLiteServer autoconnectlist option.
TIR96600	Resolved an issue where a Dymo label writer 400 printer incorrectly displayed offline messages in Citrix Virtual Apps and Desktops sessions.
TIR96517	Support to boot without a monitor—headless booting—for Wyse 3040 thin client.
TIR96587	Resolved an issue where Microsoft RD Broker agent published applications and snipping tool did not work.
TIR96554	Resolved an issue where lower versions of CredSSP protocol that resulted in **RDP PDU is corrupted** errors.
TIR96348	Improved stability in Citrix video rendering.
TIR96599	Resolved a compatibility issue that prevented the use of ELO ET2201L touch screen with ThinOS.
TIR96714	Resolved an issue where RDSH applications disappeared when minimized.

Issue number	Description
TIR96668	Improved Horizon View session reliability when using Skype and other similar applications.
TIR96586	Resolved an RDSH application focus issue.
TIR96645	Improved Citrix Receiver session Reliability user experience.
TIR96612	Issue related to selecting 3480x1600 resolution in Wyse 5060 thin client is resolved.
TIR96610	Resolved an issue preventing the use of ELO2002L multi-touch monitors.
TIR96631	Added ThinOS support for Dell Defender two-factor authentication.
TIR96677	Resolved issues preventing persistent event logging to a file server.
TIR96638	Resolved an issue where ThinOS truncated part of the RFID card causing Imprivata OneSign to associate the card to an incorrect ID.
TIR96640	Resolved a stability issue which affected ReinerSCT cyberJack e-com devices.
TIR96642	Resolved a WINS registration issue while using a wireless connection.
TIR96718	Resolved an issue where selecting Coordinated Universal Time in Wyse Management Suite changed to Casablanca time zone on ThinOS clients.
TIR96851	Added a ThinOS configuration parameter to disable RDP WebSockets. SessionConfig=RDP TsgwWebsock=no
TIR96710	SR967465508—General ThinOS stability improvements (heap free pool).
TIR96748	Resolved a stability issue where Imprivata RFID proximity card taps (Epic application) resulting in session termination.
TIR96750	SR967408834—Resolved an issue where Intel 7260 wireless module initialization is failed after upgrading ThinOS clients to 8.4 or higher in Wyse 5010 thin client.
TIR96782	Added ThinOS support for the Omnikey 5022 device.
TIR96784	General reliability improvements (conmgr).
TIR96834	Resolved an RDP application focus issue when task bar messages are displayed.
TIR96845	SR967678322—Resolved an issue where AutoSignOff=Yes Shutdown=yes do not function on Wyse 3040 thin client wireless units.
TIR96873	Resolved a sign on issue that affects password which contains the EURO symbol—€.
TIR96978	Resolved an issue where ThinOS displays the message **incorrect PIN** instead of **blocked smartcard**.
TIR96945	SR965931048—Fixed a PCoIP Horizon USB XHCI reset issue that affected several printer and scanner devices
TIR96930	Resolved an issue where an extra space is inserted in front of the IP address that is communicated to the Horizon View client.

Issue number	Description
TIR96132	SR961444036—Resolved an issue where Blast protocol session connections occasionally crash and result in blank sessions.
TIR96916	Resolved an issue where **Screensaver not found** event log message is seen when using Wyse Management Suite.
TIR97025	Resolved a ThinOS compatibility issue when using ELO Intellitouch monitors—ET2201L
TIR96223	Resolved a BIOS compatibility issue affecting Medigenic keyboards in Wyse 5060 thin client.
TIR97189	SR965329895—Resolved an issue with Citrix ICA session stability.
TIR96236	Improved PCoIP performance when reconnecting to VMware View sessions.
TIR97295	SR977614848—Resolved a Wyse Management Suite issue that result in the loss of client configurations
TIR97158	Resolved an issue where EAP-FAST authentication fails when a second user attempts to authenticate.
TIR96799	SR951522285/SR962648039—General stability improvements.
TIR97108	Resolved an issue where the client uses the last IP address after being issued a new IP address from a DHCP server.
TIR97139	Resolved an issue which caused long delays in Citrix sessions when using Imprivata OneSign.

Known issues

Table 52. Known issues

Issue number	Description	Workaround
TIR96815	Microsoft RD Gateway service stops functioning when WebSockets are enabled.	Add the following ThinOS configuration parameter to disable RDP WebSockets: SessionConfig=RDP TsgwWebsock=no

8

ThinOS 8.5_017 and ThinOS Lite 2.5_017

Priority and recommendations

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

Feature updates

This section contains information about the feature updates.

- Citrix HDX RealTime Media Engine (RTME) package is updated to version 2.4. For more information about the Citrix HDX RTME package, see docs.citrix.com.
- VMware Horizon package is updated to version 4.6.49204.
- Embedded Credential Security Support Provider (CredSSP) is updated to resolve the CredSSP Remote Code Execution vulnerability. For more information about the CredSSP Remote Code Execution vulnerability issue, see the article CVE-2018-0886 at support.microsoft.com.
- Supports display resolution of 3440 x 1440 on Wyse 3030 LT thin client.
- Supports Citrix Cloud services. For more information about Citrix Cloud services, see www.citrix.com.

NOTE:

- For more information about the ThinOS features, see the *Dell Wyse ThinOS Version 8.5 Hotfix Administrator's Guide* at Dell.com/support.
- For more information about the newly added parameters, see the latest *Dell Wyse ThinOS Version 8.5 Hotfix INI Reference Guide* at Dell.com/support.

Supported platforms

The following table provides the list of supported hardware platforms.

Table 53. Supported platforms

Platform	Image filename	BIOS filename
Wyse 3010 thin client with ThinOS	DOVE_boot	Not available
Wyse 3010 zero client for Citrix	T00_xen.bin	Not available
Wyse 3020 thin client with ThinOS—T10D	T10D_wnos	Not available
Wyse 3020 zero client for Citrix	T00D_xen	Not available
Wyse 3030 LT thin client with ThinOS	U10_wnos	U10_bios.bin
Wyse 3030 LT thin client with PCoIP	PU10_wnos	PU10_bios.bin
Wyse 3040 thin client with ThinOS	A10Q_wnos	A10Q_bios.bin
Wyse 3040 thin client with PCoIP	PA10Q_wnos	A10Q_bios.bin
Wyse 5010 thin client with ThinOS—D10D	ZD10_wnos	ZD10_bios.bin

Platform	Image filename	BIOS filename
Wyse 5010 thin client with PCoIP—D10DP	PD10_wnos	PD10_bios.bin
Wyse 5010 zero client for Citrix	ZD00_xen	ZD10_bios.bin
Wyse 5040 AIO thin client—5212	ZD10_wnos	ZD10_bios.bin
Wyse 5040 AIO thin client with PCoIP—5213	PD10_wnos	PD10_bios.bin
Wyse 5060 thin client with ThinOS	D10Q_wnos	D10Q_bios.bin
Wyse 5060 thin client with PCoIP	PD10Q_wnos	PD10Q_bios.bin
Wyse 7010 thin client with ThinOS—Z10D	ZD10_wnos	ZD10_bios.bin

Packages

The following table provides the list of the packages that are available.

Table 54. Packages

Package name	Version
FR	1.20.46089
Horizon	4.6.49204
RTME	2.4.48792
TCX	7.1.41853

Tested environment

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

Table 55. Test environment

Component	Version
Wyse Management Suite	1.2
Wyse Device Manager	5.7.2
Imprivata OneSign	5.3
Caradigm	6.3.1
NetScaler	11.1/12.0
StoreFront	3.12
Web Interface	5.4
SecureMatrix	4.1.0

Table 56. Test environment

	Windows 7	Windows 8.1	Windows 10	Linux	Windows 2008 R2	Windows 2012 R2	Windows 2016	Apps
VMware Horizon 7.0	√	√	√	√	√	√	√	√
XenDesktop 5.6	√							
XenApp 6.5					√			√
XenDesktop/ XenApp 7.15	√	√	√		√	√	√	√
Tera PCM for AWS 1.03	√ *							
RDS 2012 R2/RDS 2016	√	√	√			√	√	√

*Amazon Workspace VM operating system—Windows 7 style—is actually based on 2008 R2 RDSH.

Table 57. Test environment

XenDesktop/ XenApp	Operating system	RTME	Lync client	Skype for Business (SFB) server
7.15	Windows 7	2.4	Skype For Business 2016	Skype For Business 2015
	Windows 10	2.4	Skype For Business 2016	Skype For Business 2015
	Windows 2016	2.4	Skype For Business 2016	Skype For Business 2015

Fixed issues

The following table provides the list of fixed issues in this release:

Table 58. Fixed issues

Issue number	Description
TIR93922	Resolved an issue where a Wyse Device Manager (WDM) lock session message results in launching a new session.
TIR95856	Resolved an issue where a command to shut down a virtual machine results in a restart.
TIR96013/TIR95966	Reliability of the memory buffer is improved.
TIR95711	Resolved a low memory condition that is associated with Citrix RTME.
TIR96014	Resolved the deadlock issue when you disconnect the Citrix session.
TIR96026/TIR95971/TIR96314/TIR96179/TIR96180/ TIR96181	Reliability in using the Citrix RTME service is improved to prevent the session audio loss, resolve an issue during session disconnects, and address the RTME exit issue.
TIR95928	Resolved an issue with the Citrix video performance.

Issue number	Description
TIR95322/TIR95991	Resolved an issue where the global security policy is set to warning during system reboot after factory default.
TIR96289	Resolved an issue that results in **RTME failed to probe and commit** event log.
TIR96376	Supports 3440 x 1440 display resolution.
TIR96334	Supports the Citrix RTME 2.4 package.
TIR96286	Resolved an issue with session artifacts when you close the Skype for Business application.
TIR96292	Resolved DNS/NTP issue that results in server synchronization.
TIR96019	Reliability in using VDMMN is improved.
TIR96083	Reliability in using CTRL + ESC is improved.
TIR96084	Resolved configuration-related issues when adding or deleting certificates on an HTTPS server.
TIR96149	Resolved an issue with the classic taskbar wireless icon when you set the privilege parameter to low.
TIR96224	Resolved an issue during restart and shut down when `DisableButton` parameter is used in an admin mode.
TIR96237/TIR96033/TIR96509	Resolved an issue where Wyse Management Suite does not parse the `Device=DellCMOS` parameter.
TIR95899	Resolved an issue where the Japanese fonts are not displayed correctly on the **SelectServerList SignOn** menu.
TIR95891	Supports Citrix Cloud services.
TIR94263	Resolved an issue where the INI parameter `DiskReadOnly=yes` does not work when a hard drive is connected before you boot up the thin client.
TIR95482	Supports X/Y mouse events (Belkin F1DN102K-3 KM switch).
TIR95880	PowerMic III performance is improved in the VMware Horizon package using the PCoIP protocol.
TIR95969	Resolved an issue that prevents you to change password by using Imprivata.
TIR95813	Resolved Imprivata fingerprint reader issue when the device ID is used in EPCS applications.
TIR95989	Supports Windows 10 Canadian French keyboard layout.
TIR96043	Resolved an issue that prevents using password values of more than 24 characters or more using Imprivata.
TIR96081	Resolved an issue where network (SMB or LPD) printer mapping is limited to a single device.
TIR95508	Resolved an issue where user credentials cannot be entered again in ThinOS 802.1x PEAP.

Issue number	Description
TIR95644	Resolved Citrix SignOn failure issue by adding NetScaler `IgnoreDefaultGateway` INI option to the ThinOS PNLiteServer parameter.
TIR95679	Resolved an RTME compatibility issue that affects Vaddio AV bridge conferencing devices.
TIR95839	Resolved an RDP session reconnection issue where RDP reconnections could not detect a network disconnection before the TCP/IP timeout.
TIR95011	Resolved a black screen issue that is observed when using the Blast protocol with a SafeNet eToken 5110.
TIR96045	Resolved an issue by increasing the VMware Horizon SignOn password value to support characters more than 62 characters.
TIR95329	Improved dual monitor performance with rotated monitor configurations.
TIR96148	Resolved an issue that disconnects the Citrix session when using a Japanese keyboard.
TIR93101	Resolved the reliability issue when using the PCoIP multimedia.
TIR95299/TIR96068	Reliability in using VDCAMN is improved.
TIR96035	Resolved the connectivity issue with the VMware Blast protocol when VMware Horizon broker displays a provisioned status.
TIR96285	Reliability in using configuration manager is improved.
TIR96161	Resolved the USB unrecognized descriptor issue preventing the use of USB peripherals.
TIR96105	Resolved RDSH CredSSP vulnerability issue.
TIR96129	Resolved an issue when Citrix XenApp application does not display on the ThinOS system tray.
TIR96411	Resolved an issue where SCEP password values are displayed in clear text when it is viewed in **System Tools** is resolved.
TIR95078	Resolved an issue where wireless configuration data gets deleted during firmware upgrade.
TIR96107	Increased the NTP server list limit from 63 to 255 characters.
TIR96141	Increased the Imprivata fingerprint reader authentication duration from 30 seconds to unlimited.
TIR94399	Resolved the Wyse 3040 thin client wireless issues using the channels 52, 53 and 56.
TIR96366	Resolved the Wyse 3040 thin client wireless issue that prevents the use of `AutoSignOff=Yes` and `Reboot=Yes` INI parameters.
TIR96248	Resolved Citrix cursor inversion and display issue in Adobe Illustrator.
TIR96397	Reliability in using VDGUSBN is improved.
TIR96006/TIR95845	Resolved the ThinOS audio control issue that prevents pop-up messages (`Device=Audio Jack_Popup=No`).
TIR95632	Resolved PCoIP screen display and mouse behavior issue when changing the primary monitor.

Issue number	Description
TIR94363	Resolved the wireless memory allocation issue affecting RDSH connection stability on Wyse 3040 thin client.
TIR93558	Resolved the issue where monitors may not wake up after a scheduled reboot on Wyse 5060 thin client.
TIR95367	Reliability in using screen saver is improved.
TIR95821	Reliability in using peripherals is improved.
TIR95492/TIR96495	Resolved the mouse button combination issue observed in the Blast protocol when using the Catia application.
TIR95838	Resolved an issue where the mouse icon becomes transparent.
TIR95672/TIR95902	Resolved an issue where the displays swap when the right monitor is set to primary monitor.
TIR96477	Resolved an issue where the MTU definition results in an incorrect Ethernet MTU value.
TIR96479	Encrypted values can be used by adding the newly added parameters to the file server such as `username-enc` and `password-enc`.
TIR93661	Resolved VMware Blast protocol issue that results in Numlock/Capslock LED inversion.
TIR95819	Resolved an RDS RemoteApp focus issue when using the seamless option.
TIR96515	Supports the local Korean language.
TIR96607	Resolved an issue where wireless roaming in densely populated AP environments that results in wireless failure.
TIR96158	Resolved an issue where PH2418HT touch screen does not work when connected to Wyse 5010 thin client. However, ICA session only supports single touch, and does not support multi touch.

Known issues

Table 59. Known issues

Issue number	Description	Workaround
TIR96652	VMware Blast protocol—Trap 14 event log error occurs when you launch or reconnect the VMware session. This event results in a blank display.	There is no workaround available in this release.
TIR96236	PCoIP protocol—Roaming session between clients may extend up to 16 seconds in the VMware Windows 10 virtual machine environment. This issue affects all Teradici soft clients.	There is no workaround available in this release.
TIR96348	ICA protocol—ICA session terminates when you exit a media file during playback.	There is no workaround available in this release.
TIR95973	Wyse 3040 thin client with ThinOS and PCoIP—Monitors may not wake up when you exit the power-saving mode.	There is no workaround available in this release.

Issue number	Description	Workaround
TIR93805	ELO USB touch screen does not work on Wyse ThinOS version 8.5 operating system.	There is no workaround available in this release.

ThinOS 8.5_012 and ThinOS Lite 2.5_012

Priority and recommendations

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

Feature updates

This release note contains information about the following feature updates:

- GUI enhancement—Earlier when the connection to https file server fails in full security mode, a dialog box is displayed which prompts you to click **OK**. In this release, the feature is updated to display a tooltip at the bottom-right of the screen.
- Updates to H.264 decoder on ThinOS—The following table describes the performance of H.264 decoder in VMware Horizon sessions that use the VMware Blast display protocol:

Table 60. 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.
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.

Supported platforms

The following table lists the supported hardware platforms:

Table 61. Supported platforms

Platform	Image
Wyse 3010 thin client with ThinOS—T10	DOVE_boot
Wyse 3010 zero client for Citrix	T00_xen.bin
Wyse 3020 thin client with ThinOS—T10D	T10D_wnos
Wyse 3020 zero client for Citrix	T00D_xen
Wyse 3030 LT thin client with ThinOS	U10_wnos
Wyse 3030 LT thin client with PCoIP	PU10_wnos
Wyse 3040 thin client with ThinOS	A10Q_wnos

Platform	Image
Wyse 3040 thin client with PCoIP	PA10Q_wnos
Wyse 5010 thin client with ThinOS—D10D	ZD10_wnos
Wyse 5010 thin client with PCoIP—D10DP	PD10_wnos
Wyse 5010 zero client for Citrix	ZD00_xen
Wyse 5040 AIO thin client—5212	ZD10_wnos
Wyse 5040 AIO thin client with PCoIP—5213	PD10_wnos
Wyse 5060 thin client with ThinOS	D10Q_wnos
Wyse 5060 thin client with PCoIP	PD10Q_wnos
Wyse 7010 thin client with ThinOS—Z10D	ZD10_wnos

Fixed issues

The following are the fixed issues in this release:

Table 62. Fixed issues

CIR	Description
CIR93220	Icons display order controls for applications and desktops published using Citrix Receiver.
CIR94701	VNC port number can be defined using ThinOS.
CIR94758	General reliability is enhanced—hub_daemon.
CIR94456	DEVICE_SECURITY parameter issue is observed that results in boot failures when the parameter is defined in an INCLUDE file.
CIR89252	Support for ReinerSCT Cyberjack e-com devices.
CIR93969/CIR95622	PCoIP package extraction issue—VMware session launch failures after a firmware update.
CIR94139	Display issue is observed that affect terminal emulator application display.
CIR94214	When a VM is restarted, a window is displayed with incorrect message.
CIR94800	USB Mass Storage devices with GPT format are not recognized.
CIR94200	Support for HID Crescendo c1150 smartcard devices.
CIR94406	Crescendo 11xx Active Identity V2 profile support is added.
CIR93427	Incorrect ARP is sent after obtaining an IP address from DHCP.
CIR94286	Improved recording quality issue associated to Aten USB switch when using a Jabra PRO9460 device.
CIR94690	Functionality to define UNC paths for firmware and BIOS upgrade file locations.
CIR94860	`Screensaver` parameter lock functionality is enhanced to enable lock terminal with no defined type.
CIR94943	Event log grammar issue associated to the `SecurityPolicy` parameter is resolved.
CIR94849	Smartcard login fail with OCSP configured for domain controller kerberos certificates is resolved.
CIR94955	High resolution videos do not play with Windows Media Player in a Citrix XenDesktop session.

CIR	Description
CIR94594	3840 x 1600 monitor resolution is added in Wyse 5060 thin clients.
CIR95067	EAP-PEAP negotiation failures due to TLS version checking is resolved.
CIR95256	Sensitivity issues pertaining to DHCP option 199 is observed—Wyse Management Suite Group.
CIR95326	DHCP option 199 results in client resets to factory defaults are resolved.
CIR95008	General reliability is enhanced—Page fault callout.
CIR95315	Default ThinOS desktop wallpaper is displayed during each boot before loading the bitmap defined in the configuration file.
CIR94255	General reliability is enhanced—Wyse Management Suite agent.
CIR94216	Ability to disable WIFI scans is added.
CIR94915	Display of security warning messages on the initial boot after a reset to factory defaults is resolved.
CIR95438	Issue preventing file server access after a reset to factory defaults is resolved.
CIR95410	SCEP enrollment password limit extended from 28 to 63 characters.
CIR94595	Invert functionality of the mouse scroll wheel when using Blast and PCoIP protocols is resolved.
CIR95006	Desktop icon display controls are added when using a VMware View Broker Blast in Classic desktop mode.
CIR95019	General reliability is enhanced—HUEWEI P8.
CIR92442	Issue where the client automatically adds: 443 to the URL when connecting to an https file server is resolved.
CIR94370/CIR93368	Local Flash security is enhanced to protect ThinOS system files.
CIR95358	General reliability is enhanced.
CIR93701	Added functionality to disable `AutoSignoff=Yes` when a session connection fails.
CIR95226	Imprivata WebAPI enhancement to reduce the number of transactions to the OneSign server.
CIR95311	Changed Citrix Receiver version in Citrix monitor to display the same version in the user interface.
CIR93929	Wireless issue where DHCP renew/rebind is enabled after each roam.
CIR94913	Differentiated services do not function when using Skype.
CIR94026	The \ key on the 109 Japanese keyboard does not send a value when using Blast protocol.
CIR95634	In Wyse 3040 thin client, the wireless units do not associate to access points using channels 120, 124, and 128.
CIR95624	In Wyse 3040 thin client, the wireless roaming delay periods when roaming between access points are improved.
CIR95476	AutoStart (auto connect) fails when you are using Imprivata OneSign.
CIR95649	Drive letter mapping fails with SD card reader.
CIR95712	General reliability is enhanced—VDGUSBN.
CIR93039	Functionality to manage desktop icon ordering is added.

CIR	Description
CIR92843	Support for the Safenet SC650 smartcard.
CIR95671	General reliability is enhanced—hub_daemon.
CIR95524	The client automatically adds: 80 to the URL when connecting to an http file server.
CIR95488	General reliability is enhanced—Page fault.
CIR95450	Resolved an issue preventing NLA logon using Gemalto IDPrime.Net smartcards.
CIR94433	In Wyse 3040 thin client, 5 GHz wireless network reliability is enhanced.
CIR93303	Blast sessions freeze when thin client is idle—VMware / AppStack.
CIR93020	Users can enter credentials before the group profile is loaded.
CIR94634	Wireless reliability is enhanced.
CIR94986	The \ key is ignored when using Blast Extreme protocol.
CIR95030	Firmware upgrade affects wireless configurations.
CIR94068	In Wyse 5060 thin client BIOS support is upgraded to version 1.0E.
CIR93081	BIOS password limit extended to 15 characters.
CIR93926	Multi-Touch support is added.
CIR94400	In Wyse 3040 thin client, the screen display distorts if the monitor is turned off and then turned on.
CIR95675	Memory allocation issue results in free memory with less than 10 percent warning messages.
CIR95386	Wireless performance is improved.
CIR94785	SCEP issue while using Venafi.
CIR95727	Issues are preventing https SCEP enrollment.
CIR93244	Event log message is enhanced to improve WDM status reporting.
CIR94201	Moving the client to a new Wyse Management Suite group causes network settings to reset to factory defaults.

Packages

The following table lists the packages:

Table 63. Packages

Package name	Version
FR	1.20.46089
Horizon	4.6.47367
RTME	2.3.44433
TCX	7.1.41853

INI parameters

The following table lists the INI parameters:

Table 64. INI parameters

Parameters	Description
PRIVILEGE=[None, Low, High] [LockDown= {no, yes}] [HideSysInfo={no, yes}] [HidePPP={no, yes}] [HidePN={no, yes}] [HideConnectionManager={no, yes}] [EnableNetworkTest={no, yes}] [EnableTrace={no, yes}] [ShowDisplaySettings={no, yes}] [EnableKeyboardMouseSettings={no, yes}] [KeepDHCPRequestIP={no, yes}] [SuppressTaskBar={no, yes, auto}] [EnablePrinterSettings={no, yes}] [CoreDump={ide, disabled] [EnableNetworkSetup={yes, no}] [DisableNetworkOptions={yes, no}] [EnableSystemPreferences={yes, no, TerminalNameOnly}] [DisableTerminalName={yes, no}] [DisableSerial={yes, no}] [DisableRotate={yes, no}] [DisableChangeDateTime={yes, no}] [EnableVPNManager={yes, no}] [TrapReboot={yes, no}] [EnableCancel={yes, no}] [EnablePeripherals={keyboard, mouse, audio, serial, camera, touchscreen, bluetooth}] [FastDHCP={yes,no}] *HideWlanScan=[yes, no] *TCPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF] *UDPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF]	Default is **high**. Privilege controls operator privileges and access to thin client resources. See also CCMEnable={yes, no}. None—This level of access is typical for kiosk or other restricted-use deployment. The system setup selection on the desktop menu is disabled, and the setup submenu is not displayed. The Connect Manager is disabled by default. The Connect Manager can be enabled by using the HideConnectionManager=no option, however, the user cannot create a connection or edit an existing connection. The user cannot reset the thin client to factory defaults. Low—This access level is assigned to a typical user. The Network selection on the Setup submenu is disabled, and the Network Setup dialog box cannot be opened. The user cannot reset the thin client to factory defaults. High—Administrator access level allows all thin client resources to be available with no restrictions. A user can reset to factory defaults. **NOTE:** If None or Low is used, the Network Setup dialog box is disabled. If it is necessary to access this dialog box and the setting None or Low is not saved into NVRAM, remove the network socket and reboot. **LockDown**—Default is**no**. Yes/no option to allow lockdown of the thin client. If yes is specified, the system saves the privilege level in Flash. If no is specified, the system clears the privilege level from Flash to the default unlocked state. **NOTE:** If the thin client is set to LockDown without a High privilege level, it disables the G key reset on start up. LockDown can be used to set the default privilege of the thin client. For example • If LockDown=yes, then the privilege is saved in permanent registry. • If LockDown=no, then the privilege level is set to the default high in the permanent registry. That is, the system has a default high privilege level, which is stored in the permanent registry. • If you do not specify a privilege in either the wnos.ini file or the {username}.ini file or the network is unavailable, the setting of LockDown takes effect. It can be modified by a clause. For example, privilege=<none|low|high>lockdown=yes in a wnos.ini file or a {username}.ini file sets the default privilege to the specified level. **HideSysInfo**—Default is **no**. Yes/no option to hide the System Information from view.

Parameters	Description
	HidePPP—Default is **no**. Yes/no option to hide the Dialup Manager, PPPoE Manager, and PPTP Manager from view. **HidePN**—Default is **no**. Yes/no option to hide the PNAgent or PNLite icon from view on the taskbar. **HideConnectionManager**—Default is **no**. Yes/no option to hide the **Connect Manager** window from view. **NOTE:** As stated earlier, although the Connect Manager is disabled by default if Privilege=none, the Connect Manager can be enabled by using HideConnectionManager=no; however, the user cannot create a connection or edit an existing connection. **EnableNetworkTest**—Default is **no**. Yes/no option to enable the Network Test. **EnableTrace**—Default is **no**. Yes/no option to enable trace functionality. The active items are added to the desktop right-click menu in Privilege=Highlevel. **ShowDisplaySettings**—Default is **no**. Yes/no option to enable the Display Settings in a popup menu. **EnableKeyboardMouseSettings**. Yes/no option to enable the keyboard and mouse configuration preferences. **KeepDHCPREquest**—Default is **no**. Yes/no option to keep the same IP address that is requested from the DHCP server after a request fails and does not invoke the Network Setup dialog box. **SuppressTaskBar**—Default is **no**. Yes/no/auto option to hide the taskbar. If set to auto the taskbar will automatically hide/display the taskbar. When you use this parameter in a wnos.ini file, it is saved to NVRAM if EnableLocal is set to yes in the wnos.ini file. **EnablePrinterSettings**—Default is**no**. Yes/no option to enable printer configurations when a user Privilege=None. **CoreDump**—The option CoreDump=disabled disables the core dump function. **EnableNetworkSetup**—This option is used to enable and disable the network setup. **DisableNetworkOptions**—This option is used to enable and disable the network options. **EnableSystemPreferences**—If the optional parameter, EnableSystemPreferences=TerminalNameOnly is set with Privilege=none, then the System Preferences menu is enabled, and only Terminal Name field can be accessed. **DisableTerminalName**—This option is used to enable and disable the terminal name. **DisableSerial**—This option is used to enable and disable the serial table in peripherals.

Parameters	Description
	DisableRotate—If the optional DisableRotate=yes is set, the rotate setting in the display setup is disabled. This is only valid for C class clients because the rotation performance in C class may not be desirable. **NOTE:** If the optional EnableNetworkSetup=yes is set with Privilege={none, low}, the network setup is enabled. If the optional DisableNetworkOptions=yes is set at the same time, the options table is disabled. If the optional EnableSystemPreferences=yes is set with Privilege={none, low}, the system preferences setup is enabled. If the optional DisableTerminalName=yes is set at the same time, the terminal name field is disabled. If the optional DisableSerial=yes is set with Privilege={none, low}, the serial table in peripherals setup is enabled. **DisableChangeDateTime**—If the optional DisableChangeDateTime is set, the function of changing date and time locally is disabled. For example, if you right-click the time label in taskbar, nothing is displayed. The **Change Date and Time** button in System Preference is invisible. **EnableVPNManager**—If the optional EnableVPNManager=yes is set with Privilege={none, low}, the VPN Manager setup is enabled. **TrapReboot**—If the optional TrapReboot=yes is set, client reboots after the execution of the trap. **EnableCancel**—If the optional EnableCancel=yes is set with Privilege={none, low}, the counter down window for reboot or shutdown can be cancelled. The default value is no. For example, set the following ini, Inactive=1 AutoSignoff=yes Shutdown=yes ShutdownCounter=30 Privilege=none EnableCancel=yes. After no mouse and keyboard input in 1 minute, the system will pop up a counter down window to shut down in 30 seconds. You can cancel it. **EnablePeripherals**—If the optional EnablePeripherals is set with Privilege=none, the specified peripherals tab is enabled. The value of the option can be a list of any valid value separated with "," or ";". For Camera, Touchscreen and Bluetooth, they can be enabled only, if the devices are available. For example, Privilege=none lockdown=yes EnablePeripherals=mouse,audio,camera,bluetooth, then mouse and audio tab is enabled. If there are camera and/or bluetooth devices, the camera and/or bluetooth tab are enabled. The optional

Parameters	Description
	EnableKeyboardMouseSettings=yes can be replaced as: Privilege=none lockdown=yes EnablePeripherals=keyboard,mouse. **FastDHCP**—FastDHCP identifies the gateway first. If the gateway is same as the network before disconnection and the previous DHCP information is valid, the same information is used. The default value is yes. **HideWlanScan**—HideWlanScan is used to disable WiFi scan in lockdown mode. The default value is no. **TCPTosDscp**—TCPTosDscp is used to set TOS field for all TCP packets when it is not preconfigured by other INI settings. **UDPTosDscp**—UDPTosDscp is used to set TOS field for all UDP packets when it is not preconfigured by other INI settings.
AutoSignoff={no, yes, 2–60}* [Shutdown={no, yes}] [Reboot={no, yes}]	Default is no. AutoSignoff—Yes/no option to automatically sign out a user when the last opened session is closed. Shutdown—Default is no. Yes/no option to shut down the thin client. If shutdown is set to yes, the ShutdownCounter value is used to control the count-down before the system is turned off. Reboot—Default is no. Yes/no option to reboot the thin client. If Reboot is set to yes, the ShutdownCounter value is used to control the count down before the system is rebooted. **AutoSignOff**—AutoSignOff can configure a value from 2 to 60. This value represents the number of seconds a particular session must be active before calling AutoSignOff parameter.
SessionConfig=ALL [unmapprinters={no, yes}] [unmapserials={no, yes}] [smartcards={no, yes}] [mapdisks={no, yes}] [disablesound={no, yes, 2}] [unmapusb={no, yes}] [DisksReadOnly={no, yes}] [MouseQueueTimer={0–99}] [WyseVDA={no, yes}] [WyseVDA_PortRange=startPort, endPort] [UnmapClipboard={no, yes}] [DefaultColor={0,1,2}] [VUSB_DISKS={yes, no}] [VUSB_AUDIO={yes, no}]	**SessionConfig**—Specifies the default settings of the optional connection parameters for all sessions. **unmapprinters**—Default is **no**. Yes/no option to un-map printers. **unmapserials**—Default is **no**. Yes/no option to un-map serials. **smartcards**—Default is **no**. Yes/no option to use smartcards. **mapdisks**—Default is **no**. Yes/no option to map disks. **disablesound**—Default is **no**. Yes/no option to disable sound. If value is set to 2, the sound at remote computer is disabled. **unmapusb**—Default is **no**. Yes/no option to un-map USBs. **DisksReadOnly**—Default is **no**. Yes/no option to mount mass storage disks as read-only. **MouseQueueTimer**—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. **WyseVDA**—Default is **no**. Yes/no option to enable Virtual Desktop Accelerator for all ICA and RDP sessions. **WyseVDA_PortRange**—Sets the ThinOS VDA client port range. The port range must follow these rules:

Parameters	Description
[VUSB_VIDEO={yes, no}] [VUSB_PRINTER={yes, no}] [FullScreen={no, yes}] [Resolution={default, vga_resolution}] [DisableResetVM={no, yes}] [WyseVDAServerPort=serverPort] [FontSmoothing={yes, no}] [AutoConnect={yes, no}] [MultiMonitor={yes, no}] [EnableImprivataVC={yes,no}] [Locale=LocaleID] [SessionLogoffTimeout=seconds] [GroupSession={yes,no}] * [OnDesktop={default, all, none, desktops, applications, ondesktop_list}	1 The port range is a list of start port and end port separated by a semicolon (;) or a comma (,). 2 Both ports must be between 1 and 65535. 3 The end port must be greater than start port. For example, WyseVDA_PortRange=3000,3010, the start port is 3000, the end port is 3010. **UnmapClipboard**—Default is **no**. Yes/no option to disable clipboard redirection for all sessions. For ICA and RDP, specifies if redirecting the clipboard. This setting in wnos.ini are saved into nvram, if EnableLocal parameter is set to yes in wnos.ini. **DefaultColor**—Specifies the default color depth to use for the session 0=256, 1=High color, 2=True Color. **VUSB_DISKS, VUSB_AUDIO, VUSB_VIDEO, and VUSB_PRINTER**—Default **no**. Specifies if these USB devices are redirected to the server using TCX Virtual USB or ICA or RDP USB redirection. By default, these devices are set as local devices. **NOTE: For example, if you want to use USB disks as a network disk, you can set SessionConfig=all mapdisks=yes VUSB_DISKS=no.** If you want to use USB disks as server side device, you can set SessionConfig=all mapdisks=no VUSB_DISKS=yes. The devices are displayed in device manager of the session. **FullScreen**—Default is **no**. Specifies the default screen mode. When you use FullScreen in a Dual Screen mode, the session is displayed in span mode **Resolution**—Default is **default**. Specifies the session resolution. For example, 640 x 480 and other supported resolutions. Default sets the resolution to the native resolution of the monitor. Setting the resolution to a value smaller than the native resolution of the monitor, allows the session in Windowed mode. The resolution value cannot be higher than the native resolution. **DisableResetVM**—Default is **no**. Set DisableResetVM=yes to disable reset VM function. As default, this function is controlled by the server side is enabled including VMware View or Citrix PNA. **WyseVDAServerPort**—Sets Wyse VDA Server Port for a ThinOS VDA client. The default port is 3471. The port range must be from 1029 to 40000. For example, WyseVDAServerPort=3000, sets VDA server port to 3000 and the client connects to the VDA server using this port. **FontSmoothing**—Default is **yes**. Set no to disable font smoothing. **AutoConnect**—Default is **yes**. Set no to disable Auto Connect function. **MultiMonitor**—Default is **yes**. Sets a multiple monitor layout. Set MultiMonitor=no to disable multiple monitor layout functions. The session has the same desktop width and height with local virtual desktop size, spanning across multiple monitors, if necessary. **EnableImprivataVC**—Default is **yes**. If set to no, the Imprivata Virtual Channel is disabled. The user can use vusb redirect instead of Imprivata Virtual Channel mode to use the Rfideas or finger print device in session as server side remote device.

Parameters	Description
	[Locale=LocaleID]—Set Locale=LocaleID to set Locale in session for localization configuration to work. For information about LocaleID, see Msdn.microsoft.com/en-us/library/windows/desktop/dd318693(v=vs.85).aspx. **SessionLogoffTimeout**—Setting SessionLogoffTimeout value forces all sessions to log off when user signs off from the broker. The default value is 0 which retains the same behavior as before, and also disconnects the sessions. If you set a value, for example 30 seconds, broker sign out waits for 30 seconds for all sessions to complete logoff, then, automatically session logs off. Broker sign out continues. During the waiting process, one notice prompts for user to check whether the session stops working if something is not saved. This feature currently supports Citrix Xen broker sessions and View Broker sessions only. **GroupSession=yes**—Set to enable the function of grouping sessions and the menu item of Group Sessions is checked when you right click the desktop. The default value is no, and the original state of Group Sessions is cleared. **OnDesktop**—This parameter specifies the connections displayed on the desktop. It enhances ondesktop options for **SessionConfig=ICA** so that the VDI brokers are also compatible with ondesktop options. If the connection is not displayed in desktop, it is still added to the connection manage list. If AutoConnectList is set in the VDIServer statement, all connections configured in AutoConnectList parameter are displayed. The connections are displayed on desktop as default. The connections can be controlled using the following values: • all—display all, same as default. • none—does not display desktops. • desktops—display only desktops. • applications—display only applications. The others are handled as a ondesktop_list. For example, if you set ondesktop=word; excel, only Word and Excel applications are displayed. The ondesktop_list also supports wildcard * such as AutoConnectList parameter in VDIServer. For example, if the value is set to ondesktop=*IE*, any application that includes the string IE is displayed. For example—farm1:IE, farm2:IExplore
*device=mtouch [mult_touch={yes, no}] [mult_jitter={5-50}]	The parameter specifies the ThinOS multi-touch monitor setting. The value mult-touch=yes enables you to use multi touch devices. The default value is yes. For mult-jitter, select a larger value if you do not prefer double-click. Select a smaller value for a better user experience. The default value is 30.
ScepAutoEnroll={yes, no} AutoRenew={yes, no} InstallCACert={yes, no} [CountryName=country]	This option is to allow client automatically get certificates and renew certificates using SCEP protocol. **ScepAutoEnroll**—Set this keyword to yes to enable client's functionality to automatically obtain certificate. Set **AutoRenew**—Set this keyword to yes to enable certificate auto renew. Client only tries to renew certificates requested either

Parameters	Description
[State=state] [Locality=locality] [Organization=organization_name] [OrganizationUnit=organization_unit] [CommonName=common_name] [Email=email_address] KeyUsage=key_usage KeyLength={1024, 2048, 4096 } [subAltName=subject_alt_name_list] RequestURL=scep_request_url CACertHashType={MD5, SHA1} CACertHash=CA_HASH_VALUE [EnrollPwd=enrollment_password] [EnrollPwdEnc=encrypted_enrollment_password] [ScepAdminUrl=scep_administrator_page_url] [ScepUser=scep_enrollment_user] [ScepUserDomain=scep_enrollment_user_domain] [ScepUserPwd=scep_enrollment_user_password] [ScepUserPwdEnc=encrypted_scep_enrollment_user_password]	manually or automatically through SCEP from this client, and the renewal is performed only after a certificate's 1/2 valid period has passed. Set **InstallCACert**—Set this keyword to yes to install the root CA's certificate as trusted certificate after successfully getting a client certificate. **CountryName, State, Locality, Organization, OrganizationUnit, CommonName, Email**—These keywords together compose the subject identity of the requested client certificate. Country Name should be two letter in uppercase, other fields are printable strings with a length shorter than 64 bytes, and email_address should have a '@' in it. At least one of the above fields must be configured correctly to form the client certificate's subject identity. **KeyUsage** —This option is to specify key usage of the client certificate and should be set to a digitalSignature, keyEncipherment or both using a ';' concatenating these two as digitalSignature;keyEncipherment. **KeyLength**—This option is to specify the key length of the client certificate in bits, must one of the value in the list. **subAltName**—This option is to specify the client certificate's subject alternative names. It is a sequenced list of name elements, and every element is either a DNS name or an IP address. Use ';' as delimiter between them. **RequestURL**—This option is to specify the SCEP server's service URL. This field must be set correctly. The default protocol for SCEP service is HTTP and data security is ensured by SCEP itself. You can also add the prefix https://, if SCEP service is deployed on HTTPS in your environment.* **CACertHashType**—This option is the hash type used to verify certificate authority's certificate. This option must be set to MD5 or SHA1 or SHA256.* **CACertHash**—This is the hash value used to verify certificate authority's certificate. Client will not issue a certificate request to a SCEP server and cannot pass certificate chain checking through a valid certificate authority. **EnrollPwd** or **EnrollPwdEnc**—These keywords are used to set the enrollment password from a SCEP administrator. **EnrollPwd** is the plain-text enrollment password and **EnrollPwdEnc** is the encrypted form of the same enrollment password. Use only one of these two fields to set the used enrollment password. As a substitute of using EnrollPwd or EnrollPwdEnc to directly specify an enrollment password, client allows using a SCEP administrator's credential to automatically get an enrollment password from a Windows SCEP server. In this case, the **ScepUser**, **ScepUserDomain**, **ScepUserPwd** (or ScepUserPwdEnc, in encrypted form instead of plan-text) are used to specify the SCEP administrator's credential, and ScepAdminUrl must be set correctly to specify the corresponding SCEP admin web page's URL. If neither EnrollPwd nor EnrollPwdEnc is set, client will try to use these set of settings to automatically get an enrollment password and then use that password to request a certificate. If communication security is necessary in your environment during this phase, please add https:// as the prefix for ScepAdminUrl to use HTTPS instead of the default HTTP protocol.

Parameters	Description
	Use ScepAutoEnroll=no AutoRenew=yes to only enable SCEP auto renew; all other parameters are not needed if ScepAutoEnroll is set to no. **NOTE: SCEP server's URL must be an HTTP link. Do not add protocol prefix to RequestURL and ScepAdminURL.**

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

10

Upgrading firmware

Downloading the installation file

1 Go to www.dell.com/support.

2 In the **Enter a Service Tag, Serial Number, Service Request...** field, type the Service Tag or the model number of your device, and press Enter or click the search icon.

3 On the product support page, click **Drivers & downloads**.

4 Select the appropriate operating system.

5 From the list, locate the file entry and click the download icon.

Firmware upgrade

Firmware upgrade is the process of updating your existing ThinOS firmware version to the latest version. To upgrade the ThinOS firmware, use any of the following:

- File Transfer Protocol (FTP) Windows server
- HTTP/HTTPS Windows server
- Dell Wyse Management Suite

NOTE: Ensure that you are enrolled in our Software Maintenance Program and are eligible to receive new versions of ThinOS software and subsequent releases of corresponding documentation uploaded on Dell Digital Locker.

IMPORTANT: To avoid uncertain issues, ensure that when you upgrade your firmware, you do not skip versions.

Table 65. Firmware images

Platform	ThinOS	ThinOS with PCoIP
Wyse 3010 thin client	DOVE_boot	Not available
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

Table 66. BIOS binary files

Platform	BIOS binary filename
Wyse 3010 thin client	Not available
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

Table 67. 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.
FR.i386.pkg	Upload the new package to central configuration, and configure the INI parameter for update this package.
TCX.i386.pkg	Upload the new package to central configuration, and configure the INI parameter to update this package.

NOTE:

- For information about the ThinOS build number, package versions, and BIOS versions, see the latest *Dell Wyse ThinOS Release Notes*.
- To downgrade the ThinOS firmware, ensure that you set the INI parameter Autoload=2, and follow the procedure using the FTP server.

Firmware upgrade using FTP server

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

Installing the Windows IIS creates the directory **C:\inetpub\ftproot**, which is known as the FTP root. In the **ftproot** directory, create a folder **wyse** and a sub folder **wnos**. The directory structure must read as **C:\inetpub\ftproot\WYSE\wnos**.

To upgrade the ThinOS firmware using FTP server:

1 Ensure that you have downloaded 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.

2 Place the extracted firmware files in the **C:\inetpub\ftproot\WYSE\wnos** folder, and the packages to **C:\inetpub\ftproot\WYSE\wnos\pkg** on your FTP server.

3 Create a wnos.ini text file (using a text editor) in the **C:\inetpub\ftproot\WYSE\wnos** folder with the following INI parameters:

```
Autoload=2 loadpkg=1 Addpkg=TCX,FR,horizon
```

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, FR, Horizon, and TCX. 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.

4 Save the wnos.ini file.

5 On the ThinOS client desktop, navigate to **System Setup** > **Central Configuration** > **General**.

6 In the **General** tab, enter the IP address of the FTP server or directory. For example: **150.00.0.260/wyse**. The **Username** field must have the value `Anonymous` and the **Password** field is already pre-configured.

NOTE:

- If there is no default password or if the password is changed, then you must set your password. For example, abe@abc.com.

  You can also reset the thin client to factory default settings. When you reset the thin client to factory default settings, the anonymous user is configured with the default password. However, you need to reconfigure the thin client.

- 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.

7 Click **OK**.

8 Restart the thin client and wait until the auto-installation of packages is complete.

To verify that the thin client is upgraded, on the ThinOS desktop, navigate to **System Information** > **General**, and check the System Version.

Firmware upgrade using HTTP or HTTPS

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

1 Ensure that you have downloaded 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.

2 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 HTTP or HTTPS server.

3 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=TCX,FR,horizon
```

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, FR, Horizon, and TCX. 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.

4 Save the wnos.ini file.

5 On the ThinOS client desktop, navigate to **System Setup** > **Central Configuration** > **General**.

6 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.

7 Click **OK**.

8 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. For more information, see the latest *Dell Wyse Management Suite Administrator's Guide*.

Ensure that your ThinOS clients are registered to Wyse Management Suite. For more information, see the latest *Dell Wyse ThinOS 8.5 Administrator's Guide*.

To upgrade the ThinOS firmware using Wyse Management Suite:

1 Ensure that you have downloaded the latest ThinOS firmware and ThinOS packages that corresponds to your thin client model.

2 Log in to Wyse Management Suite using valid credentials.

3 On the **Apps & Data** page, in the **OS Image Repository** section, click **ThinOS**.

4 Click **Add Firmware File**.

The **Add File** dialog box is displayed.

5 Browse and select the downloaded firmware file. Enter an appropriate description.

6 Click **Upload**.

The ThinOS firmware file is uploaded, and the firmware file is listed on the **Apps & Data - ThinOS OS Image Repository** page.

7 Select the check box that corresponds to your ThinOS firmware file.

8 On the **Groups & Configs** page, select a custom group, and click **Edit Policies** > **ThinOS**.

The **Select ThinOS Configuration Mode** screen is displayed.

9 Click **Advanced Configuration**.

10 In the **Device Configuration** pane, click **Firmware Upgrade**, and then click **Configure this item**.

11 From the **Platform type** drop-down list, select your thin client model.

12 From the **Firmware to auto deploy** drop-down list, select the firmware file that corresponds to your thin client model.

13 Click **Save & Publish**.

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

11

Resources and support

Accessing documents using the product search

1 Go to www.dell.com/support.

2 In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, `Wyse 3040 thin client` or `Wyse ThinOS`.

A list of matching products is displayed.

3 Select your product and click the search icon or press Enter.

4 Click **Manuals & documents**.

Accessing documents using product selector

You can also access documents by selecting your product.

1 Go to www.dell.com/support.

2 Click **Browse all products**.

3 Click **Thin Clients**.

4 Click the desired category, either **Wyse Hardware** or **Wyse Software**.

5 Click the desired product.

6 Click **Manuals & documents**.

Additional resources

Table 68. Additional resources

Resource	Content
Dell support website—www.dell.com/manuals.	Administrator's Guide, INI Reference Guide, and Release Notes.
Citrix support website—docs.citrix.com.	Documentation for Citrix software.
VMware support website—docs.vmware.com.	Documentation for VMware software.
Microsoft support website—support.microsoft.com.	Documentation for Microsoft software.

12

Contacting Dell

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for technical support or customer service issues, see www.dell.com/contactdell.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.