Dell Pro 24 All-in-One

QC24251 Reimaging Guide for ThinOS 10



Notes, cautions, and warnings

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

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

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

© 2025 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Chapter 1: Installation overview	4
Chapter 2: Introduction	5
Chapter 3: Updating or resetting the BIOS	6
Clearing CMOS settings	6
Trusted Platform Module (TPM) security	6
Chapter 4: Downloading and installing ThinOS 10 from a USB drive using the De Recovery Tool	7
WMS Configuration Known behavior	19
Chapter 5: Reinstalling drivers and applications	20
Displaying drivers and applications on your computer	
Chapter 6: Getting help and contacting Dell	21

Installation overview

- CAUTION: This reimaging guide is designed for system administrators. Do not attempt to reimage your computer if you are not an administrator or if you are unsure of the procedures. Failure to follow instructions may result in permanent data loss.
- **NOTE:** The information that is provided in this guide is only applicable to computers with the ThinOS 10 operating system installed.
- **NOTE:** The minimum requirements for ThinOS 10 are 8 GB of RAM and 32 GB of storage. It does not support the I7 processor.
- **NOTE:** The Dell operating system recovery image is available for the original operating system that was shipped with the Dell computer.
- () NOTE: Dell Technologies recommends that you download and install the device drivers from the Dell Drivers & Downloads website. Installing device drivers from a non-Dell website can cause computer performance issues or corrupt operating system files. It can also cause blue screen errors, unexpected shutdowns, or infect your computer with malicious software.

Use the Dell OS Recovery Tool to create a USB recovery drive that can be used to reinstall the version of operating system installed in the computer.



Introduction

CAUTION: This reimaging guide is designed for system administrators. Do not attempt to reimage your computer if you are not an administrator or are unsure of the procedures. Failure to follow instructions may result in permanent data loss.

(i) NOTE: The information that is provided in this guide is only applicable to computers with ThinOS 10 installed.

Reimaging is the process of removing all software on the computer and reinstalling the removed software. Reimaging is required when software in the computer is corrupted or damaged. It can also be used as a means of removing harmful and malicious software in your computer. This reimaging guide provides the steps that are required for reimaging your computer.

This guide assists you in installing Dell Technologies-recommended software stack and settings, drivers, and applications, which are tested and validated on the computer. The installation of the listed drivers and applications as described in the guide enhances the optimal performance of your computer.

Dell Technologies also provides drivers and applications that are not included with the operating system. These drivers are required to enable the following solid-state drives (SSDs):

- 256 GB PCle SSD
- 512 GB PCIe SSD
- 1024 GB PCIe SSD
- 2048 GB PCIe SSD and larger capacity size PCIe SSDs

It is always recommended to reimage on a newly installed operating system and not from any previous image-build. Ensure that the BIOS settings, including SATA configurations and modes, are set appropriately and use the latest drivers and applications when reimaging the computer.



Updating or resetting the BIOS

Clearing CMOS settings

If flashing your computer with the latest BIOS update results in your computer being unable to boot, a BIOS reset is necessary. Clearing the CMOS settings will reset the BIOS to factory settings. For more information about clearing the CMOS settings, go to Dell Support Site and see your computer's *Owner's Manual*.

Trusted Platform Module (TPM) security

TPM must be enabled in the BIOS setup program for it to be deployed on the computer. Follow these steps to enable and configure the TPM:

- 1. Turn on or restart your computer.
- **2.** Press F2 when the Dell Technologies logo is displayed on the screen to enter the BIOS setup program. The BIOS setup program is displayed.
- 3. On the left pane, select **Security**.
- 4. Select or clear any of the following options to enable or disable it, respectively:
 - TPM state (Enabled or Disabled):
 - **Enabled**: The BIOS will enable the TPM during Power-On-Self-Test (POST), and it can be accessed by the operating system.
 - **Disabled**: The BIOS will not enable the TPM during Power-On-Self-Test (POST), and it cannot be accessed by the operating system.
 - TPM 2.0 security On: The TPM is enabled and activated.
 - Clear: The BIOS clears the information that is stored in the TPM.
- 5. Save the settings and exit.

Downloading and installing ThinOS 10 from a USB drive using the Dell OS Recovery Tool

- 1. Download Dell OS Recovery Tool.
- 2. Run the .exe file on the device to be used to create the USB drive. The Dell OS Recovery Tool Application installer opens.
- 3. Click INSTALL.
- 4. After the installation is complete, open Dell OS recovery Tool.
- 5. Select SWITCH TO ADVANCED RECOVERY displayed at the bottom of the tool.

OS Recovery Tool		
Automated Recovery	Step 1: Select a computer	
Welcome, Dell	This computer	Another computer
Having trouble with your system?	President 2020 Towar	Service Tag/Express Service Code
Start by selecting the computer you'd like	Service Tag	Enter service tag Q
NOTE:		
You'll need a USB with 16 GB of	_	
space available. Existing content will be deleted.		
0-0-0-0	SWITCH TO ADVANCED RECOVERY	CANCEL NEXT

Figure 1. Dell OS Recovery Tool

6. In Select an OS image, browse to the ISO file that you downloaded from the DownloadThinOS ISO image section and click NEXT.

OS Recovery Tool					
Advanced Recovery Welcome, Dell. This app will help you recover and install your OS Image. Get started by selecting which device you want to create a recovery key to support.	Select preference Select an OS image Browse CWSers\DeRDesktop\ThrrOS10_2502_11.iso	0 Q	Select from available OS images For this computer For another computer		
	SWITCH TO AUTOMATED RECOVERY			NEXT	

Figure 2. Upload the ISO file

7. Select the USB drive that you want to format from the $\boldsymbol{USB}\ \boldsymbol{drive}\ dropdown.$

NOTE: Some special USB drives do not support ThinOS ISO image by default. You can change the **Partition Style** and burn the operating system again.

- 8. User can select GPT or MBR option in the Partition Style.
- 9. Check the box "I understand that the selected drive will be reformatted, and existing data will be deleted".
- 10. Click BURN OS.

OS Recovery Tool		
Advanced Recovery We'll walk you through the process of downloading and saving the software you'll need to recover your computer. Insert a rewritable USB drive with 16 GB of space available.	Step 1: Select USB drive USB drive D: SanDisk SanDisk 3.2 Gen1 USB Device, DELLRESTORE, 32GB Partition Style GPT QPT I understand that the selected drive will be reformatted and existing data will be deleted.	
	Recovery Image \\100.106.190.10\ethos-t10\Build\2502-0020\ThinOS10_2502_20.iso	
@ —•	X SWITCH TO AUTOMATED RECOVERY GO BACK	BURN OS
	Advanced Recovery We'll walk you through the process of downloading and saving the software you'll need to recover your computer. Insert a rewritable USB drive with 16 GB of space available.	Advanced Recovery Step 1: Select USB drive We'll walk you through the process of downloading and saving the software you'll need to recover your computer. Insert a rewritable USB drive with 16 GB of space available. GPT I understand that the selected drive will be reformatted and existing data will be deleted. Recovery Image \\100.106.190.10\ethos+10\Build\2502-0020\ThinOS10_2502_20.iso

(i) NOTE: Once the burn OS process is completed, the Build is stored in USB drive.

- **11.** Remove the USB drive and connect it to the powered-off device, on which you plan to install ThinOS.
- **12.** Switch on the computer and press F2 at boot up for BIOS page.

- 13. Most of the Dell devices have a password protected BIOS. Enter the BIOS password if prompted.
- 14. Click **UNLOCK** on the Admin Password button and input the required password (The default password for most Dell Thin client is "Fireport", but this will be different if device was enrolled to WMS and can be found in the WMS console).

(i) NOTE: If no BIOS password is set, the "UNLOCK" option will not appear on the Admin Password button.

BIOS Setu	qu					
And in case of the local		Overview				
Advanced Help Text Setup Orr ON	Admin Password D UNLOCK	OptiPlex 3000 Thin Client	BIOS Version 1.12.0	Service Tag 5739553	Asset Tag (None)	Manufacture Date (None)
Overview			Ownership Date	Express Service Code	Ownership Tag	Signed Firmware Update
Boot Configuration						Enabled
Integrated Devices		Admin Unlock				
Storage						Current Clock Speed
Display						3.30 GHz
Connection Power		The admin password is	s set on this computer. This oper	ration is not allowed until correct a	dmin password is entered.	
Security						Processor L3 Cache 4096 k8
Passwords						40,00 %0
Update,Recovery						
System Management						
Keyboard Pre-boot Behavior		57395S3-8FC8				
Virtualization Support		5755556666				Memory Channel Mode
Performance						Dual
SystemLogs					OK Cancel	
						_
		DEVICES	Video Controller Intel UHD Graphics	Video Memory 8128 MB	Wi-Fi Device Intel Wireless	Native Resolution 1920 by 1080
			and one of spring	0120 MD	and modes	1100,1000
			Video BIOS Version	Audio Controller	Bluetooth® Device	LOM MAC Address
About			10101041	DAVEAU ATTEND	CONTRACT.	ALCOLOGICATE. TO
		LOAD DEFAULTS	APPLYCHANGES	charges were made		EXIT

Figure 4. Unlock BIOS screen

15. Navigate to the Integrated Devices section on the BIOS menu and ensure that Enable USB Boot Support is enabled.

and a second second second	Interneted Devices		Q	Ê
	Integrated Devices		SEARCH	VIEW #
Nunced Point Admin Password ON	Date/Time Date This option controls the system date.Changes to the date take effect immediately.Date in MM/DD/YYY format. 7 17 2024 Audio Enable Audio Use this setting to switch all integrated audio On/Off, or enable/disable the microphone and Image:			
ualization Support formance tern Logs	 Enable Microphone Enable Internal Speake USB Configuration When USB Boot Support is enabled, bootable USB mass storage devices (such as HDD, flash functional in an OS environment. If disabled, the bootable USB mass storage devices are pre functional in an OS environment. Enable Front USB Ports Enable Rear USB Ports Front USB Configuration 	h drive, CD/DVD) can boot through the boot sequence or boot menu. USS		2



Phys. 2002 Theory State	Integrated Devices	Q	ŝ
dvanced Help Text Admin etup Password	Date/Time	SEARCH	VIEW A
On ON Conversion	Date Time This option controls the system date Changes to the date take effect immediately.Date in MM/DD/YWY format. This option controls the system time.Changes to the time take effect immediately.Date in HH/MM/SS 24 Hour format. You can also switch between 12H or 24H 7 17 2024 9 45 50 12H 24H		
play			
wer curity	Audio		
swords	Enable Audio		
date,Recovery	Use this setting to switch all integrated audio On/Off, or enable/disable the microphone and the internal speaker separately.		
tem Management board			
boot Behavior	C on		
ualization Support formance	Enable Microphone Enable Internal Speaker		
tem Logs	USB Configuration		
	When USB Boot Support is enabled, bootable USB mass storage devices (such as HDD, flash drive, CD/DVD) can boot through the boot sequence or boot menu. USB functional in an OS environment. If disabled, the bootable USB mass storage devices are prevented from booting through the boot sequence and boot menu, but USE functional in an OS environment. Image: Comparison of the compa		
	Front USB Configuration		

Figure 6. Enable USB Boot Support

16. Navigate to the Security section on the BIOS menu and ensure that Start Data Wipe option under Data Wipe on Next Boot is set to ON.

BIOS Setup			
Section 200 Tex Days	Security	Q	÷
Advanced Help Text Admin Setup Password ON ON	and report intrusions during POST but do not display any detected intrusion during POST	SEARCH	VIEW ALL
Overview Boot Configuration Integrated Devices Storage Display Connection Power Security Passwords	SMM Security Mitigation SMM Security Mitigation This option enables or disables additional UEFI SMM Security Mitigation protections. The operating system can use this feature to help protect the secure environm virtualization based security. Enabling this feature provides additional UEFI SMM Security Mitigation protections. However, this feature may cause compatibility issues or loss of functionality wit applications. OFF		
Update.Recovery System Management Keyboard Pre-boot Behavior Virtualization Support Performance System Logs	Data Wipe on Next Boot Start Data Wipe If enabled, the BIOS will queue up a data wipe cycle for storage device(s) connected to the motherboard on the next reboot. Image: OFF WARNING: This Secure Wipe Operation will delete information in a way that it cannot be reconstructed.		
About	Absolute® Absolute® This field late was Eastle. Disable as Remonantly. Disable the DIOC module interface of the entired Absolute Desistance Module coming from Absolute®. Software LOAD DEFAULTS APPLY CHANGES 1 changes were made		EXIT

Figure 7. Data Wipe Screen (ON)

17. A pop-up message appears on the BIOS screen to confirm if you want to wipe the data. Select OK.

BIOS Setup			
patter and for the	Security	Q	5
Advanced Help Text Admin Setup Password	and report intrusions during POST but do not display any detected intrusion during POST by	SEARCH	VIEW ALL
verview to Configuration tregrated Devices torage	SMM Security Mitigation Data Wipe e secure environm	nent created by	
Display Connection Poever Security Deasword's Update.Recovery System Management Keyboard Pre-boot Behavior Virtualization Support Preformance System Logs	Data Wipe of functionality will be a wipe operation on ALL internal storage devices. of functionality will be erased. Do you want to continue this operation? Abort OK	th some legacy	r tools and
About	This Secure Wipe Operation will delete information in a way that it cannot be reconstructed. Absolute® LOAD DEFAULTS APPLY CHANGES things were made		EXIT

Figure 8. Data Wipe Screen (Select OK)

18. The Data Wipe pop-up message asks if you want to cancel or proceed with the operation. Select **NO**.

BIOS Setup		
and the second second		
Advanced Help Text Admin Setup Password	and report intrusions during POST but do not display any detected intrusion during POST	
verview oot Configuration	CMM Convity Mitination	
ntegrated Devices Storage	Data Wipe	e secure environment created by
Display Connection	Data Wipe	of functionality with some legacy tools and
Prover Passwords UpdateRecovery System Management Kysband Pre-boot Behavior Vistualization Support Preformance System Logs	WARNINS: If you continue with this operation all the data on ALL internal storage devices will be erased. You will not balk to recover this data! Do you want to cancel this operation? Yes No	
	Absolute®	
About	AbsoluteS LOAD DEFAULTS APPLY CHANGES Changes were made	 Exit

Figure 9. Data Wipe Screen (Select NO)

19. In the Security section on the BIOS menu, enable the TPM Clear option if disabled. Then select Yes.



Figure 10. TPM Clear option is available

-		Q	Êr
	Security	SEARCH	VIEW ALL
dvanced Help Text Admin etup ON ON Password	This option lets you control whether the Trusted Platform Module (TPM) Storage Hierarchy is available to the operating system. Disabling this setting restricts the storing owner data.		
erview			
ot Configuration egrated Devices	Clear TPM : boot. When this	option is uncho	akad the
rage		option is unche	cked, the
play	Clear TPM		
nnection			
ver urity	Data encrypted with keys stored in the TPM will be lost. Are you sure you want to clear all keys from the TPM?	ill not take effec	t in the
swords	Yes No		
ate,Recovery	Tes NO		
tem Management			
board			
boot Behavior	ssuing the Clear	command. when	i disabled,
ualization Support			
ormance			
tem Logs			
	This neid controls the chassis infrusion feature.		
	A chassis intrusion has been detected. Select "Clear Intrusion Warning" to acknowledge and clear this event. The system will then be armed to look for future sec	irity breaches.	
	Disabled Enabled On-Silent Disable the intrusion detection feature and report intrusions during POST Enable the intrusion detection feature but do not display any detected intrusion during POST Enable the intrusion detection feature but do not display any detected intrusion during POST		
ut			
oout	LOAD DEFAULTS APPLY CHANGES 0 changes were made	_	

Figure 11. Enable TPM Clear option



Figure 12. TPM Clear is enabled

20. If the **TPM Clear** option is grayed out in the BIOS, it indicates that Intel Platform Trust Technology (PTT) is enabled by default. Only one of these trust technologies (TPM or PTT) can be active at a time. Please go to the next step.

Dell	BIOS Setu	р			
-	Concernant Concernant		Security	Q	ця В
Advanced	Help Text	Admin		SEARCH	VIEW ALL
Setup	_	Password	TPM 2.0 Security		î
ON 💽	ON 🚺		TPM 2.0 Security On		- 1
Overview			Select whether or not the Trusted Platform Module (TPM) is visible to the OS.		- 1
Boot Config	uration		ON		- 1
Integrated D	levices		Attestation Enable		- 1
Storage Display			This option lets you control whether the Trusted Platform Module (TPM) Endorsement Hierarchy is available to the operating system. Disabling this setting restricts t TPM for signing and signature operations.	ne ability to u	se the
Connection Power			C ON		
Security			Key Storage Enable		
Passwords Update,Reco	overy		This option lets you control whether the Trusted Platform Module (TPM) Storage Hierarchy is available to the operating system. Disabling this setting restricts the ab storing owner data.	lity to use the	TPM for
System Mar	nagement		C ON		
Keyboard Pre-boot Be	hand and		SHA-256		
Virtualizatio	n Support		When this option is checked, the BIOS and the TPM will use the SHA-256 hash algorithm to extend measurements into the TPM PCRs during BIOS boot. When this op BIOS and the TPM will use the SHA-1 hash algorithm.	ion is unchec	ked, the
System Log					
			Clear		
			This setting clears the TPM owner information, and returns the TPM to the default state. Changes to this setting will be latched in BIOS after clicking "apply", but will n TPM until after exiting the BIOS setup menu.	ot take effect	in the
			OFF		
			PPI Bypass for Clear Commands		
			This option controls the TPM Physical Presence Interface (PPI). When enabled, this setting will allow the OS to skip BIOS PPI user prompts when issuing the Clear con this setting will require user physical presence interaction to follow instruction from BIOS.	nmand. When	disabled, v
About			LGAD DEFAULTS APPLY CHANNEES 0 changes were made		EXIT

Figure 13. TPM Clear option is greyed out

 $\ensuremath{\textbf{21.}}$ Exit the BIOS settings. Select $\ensuremath{\textbf{Yes}}$ to save the changes.

BIOS Setup					
atta ten ha taa	Security			Q	
dvanced Help Text Admin etup Password ON ON		and report intrusions during POST	but do not display any detected intrusion during POST	SEAR D	CH VIEW ALL
verview	SMM Security Mitigation				
ot Configuration legrated Devices	SMM Security Mitigation				
orage				secure environment creat	od by
splay				secure environment creat	cuby
nnection	Warning			functionality with some le	egacy tools and
wer					
urity	Do you want to save changes?				
swords					
date,Recovery					
item Management /board					
board boot Behavior					
ualization Support			Yes No Cance	4	
formance					
stem Logs					
	WARNING! This Secure Wine Operation will	delete information in a way that it cannot be reconstruc	tod		
	This secure wipe operation will	delete information in a way that it cannot be reconstruc-	teu.		
	Absolute®				
	Absolute®				
	Absolute®				
ut					
	LOAD DEFAULTS	APPLY CHANGES 2 changes were made			EXIT

Figure 14. Exit the BIOS settings

22. Dell Security Manager screen is displayed. Select **Continue** to erase the data.

Dell Security Manager You have chosen to perform the Data Wipe operation on ALL internal storage devices. If you continue with this operation all the data on these storage devices will be erased. Do you want to continue this operation?
storage devices. If you continue with this operation all the data on these storage devices will be erased.
Continue Cancel Use arrow keys to select an option and press Enter Use Volume Up/Down to select an option and press 'Home' button Dell

Figure 15. Erase the data

 $\ensuremath{\textbf{23.}}$ In the Dell Security Manager screen, select $\ensuremath{\textbf{ERASE}}$ to erase the data.



Figure 16. Select Erase

24. Select OK to reboot the computer.

Dell Security Manager	
Data Wipe Completed Successfully.	
Press 'OK' to reboot the system.	
OK Use arrow keys to select an option and press Enter Use Volume Up/Down to select an option and press 'Home' button Dell	

Figure 17. Select OK to reboot

25. During reboot, press F12 at boot up and hold it until the Dell logo appears and **Preparing one-time boot menu...** is displayed in the top-right corner. The boot menu will then open.

26. In the boot menu, select the USB drive from the UEFI Boot Devices list.

(oeu)			SERVICE TAG BIOS REVISION FBGF434 1.15.0
One-Time Boot Settings Control the boot flow for the SupportAssist OS Recovery Tool.	Pre-Boot Tasks Change important BIOS settings on your system, configure ho	w your device works and troubleshoot issues using this interfa	ce.
NOTE: Once a system and/or admin password is set, the system will always prompt for system and/or admin password during boot.	BIOS SETUP Configure BIOS options and control how your system functions.	DIAGNOSTICS Run system tests to identify any issues.	BIOS UPDATE Search for and install the latest BIOS updates from various services.
JEFI Boot Devices	BIOS Flash Update - Remote	Device Configuration	
UEFI USB SanDisk 3.2Gen1 04018248fba447ae5d94cdaf8b9a3488d 8048665b3271d82351ca77d2941eba10 83100000000000000000000823f68ecff1 d8418a955810710aa61b9	BIOS and Firmware Update Over-the-Air	B nfigure device settings	
LUEFI HTTPs Boot (MAC:D0460C80DF91)			
			EXIT

Figure 18. UEFI Boot Devices – USB (Select)

27. After selecting the USB key, the device will reboot automatically, and the installation will begin.

0	Dell ThinOS 10 Welcome to the most secure Thin Client Operating System	
	Installing Time remaining 90 seconds	
ThinOS is the meet modern	exclusive VDI client solution, meticulously engineered and crafted to customer needs. With its seamless deployment and robust security, it's for virtual environments.	

Figure 19. Dell ThinOS 10 installation

28. After Installation, the OOBE screen is displayed. Click -> button to proceed to the next page.

(i) NOTE: If a network cable is connected, the page will automatically advance once the IP address is obtained.

(i) NOTE: If WMS (Wyse Management Suite) discovery is configured, the device will check in automatically, and the OOBE screen will not be displayed.

29. In the Dell Technologies page, click the -> to go to the Review License Agreement page.



Figure 20. Dell Technologies screen

30. In the Review License Agreement page, select **I have reviewed all license agreements** and then click **>** button to proceed to the next page.

Dell ThinOS 10 Welcome to the most secure Thin Client Operating System. Let's get started.	
Review License Agreement	
Dell Technologies Citrix JVDI HID TeamsVDI WebexMeetings	
Congratulations on your new Dell purchase!	
Your purchase and use of this product is subject to and governed by Del's applicable Terms of Sale and End User License Agreement, which are each presented below in the following order:	
U.S. Consumer Terms of Sale	
Commercial Terms of Sale	
End User License Agreement In addition, please take note of the important Safety Information.	
In inductor, please was note or the implication, sately intermitted. By the act of clocking -1 accessing the plane is a steely intermitted in the foregoing terms and conditions and achievelogies that you have read and understood the Safety Information. For the available of disade, to the extern that Deal is doneed under applicable lies to have accepted an offer by your (a) Del hereby objects to and rejects all additional or inconsistent terms that may be constained in any purchase order or other documentations undertained by you is concerning the order, and (b) Del hereby conditions its acceptance on your assent that the foregoing terms and terms and become the set anticherotexter.	
I have reviewed all license agreements	



31. The QR Code Scan page is displayed.

			ell ThinOS 1 coure Thin Client Operating Sy			
QR Code Scan Optional	Language	O Keyboard	O Time Zone	O	Management Optional	Gateway Optional
		Scan Yo	ur QR Code for Auto-config	guration		
		More in	nformation about how to get a QR cos	50 ©		
			Skip >			-
Light OD Dark		Pre	ess Ctrl + Esc to skip initial configuratio	n	D	BLL Technologies

Figure 22. OOBE Screen

32. Press **Ctrl + ESC** to enter the computer.

A # 1 /	5 340		14
of the state of the			120 Mary
The Art of	States States	A A A A A A A A A A A A A A A A A A A	10 100
	ALL DE CARA	AND CONT	
	AL PROPERTY AND	A CAL	
6.02.3			- 15 E
in the second seco	OPPL		Ser. 17
	Please login to your Citrix Virtual Desktop		2
	Username Please enter username		1
	Password	and wall the	1 1
	Please enter password	A Start Start	
	Domain ranjith ~		10 1 1. 10 Ch
	Please enter your credentials		16.
\$		at 1 in the	151
0	Login	Maria Maria	Frank
7		11/1/4/2014	30
↔		33.1	
December 10		ALL	2011
*	1	The second state	and a state of the
0	and the second sec	C. A. Barrieland	250 20
Ratine	Ser Balling	Alle Martine	and the second

Figure 23. Desktop Screen (ThinOS 10)

WMS Configuration

Once the device is registered to WMS, push the policy from ThinOS 10.X configuration.



Figure 24. WMS configuration

Known behavior

- 1. If the device does not go to the installation screen after selecting the USB (and instead boots to HTTPS or encounters a security error), disable the **Secure Boot** in the BIOS.
- 2. After a successful installation, if the device fails to boot into ThinOS 10 (and instead boots to HTTPS or encounters a security error), disable the **Secure Boot** in the BIOS.
- 3. Devices with an integrated graphics card may experience UI distortion issues after installation.
- **4.** Installation time is 10 to 15 minutes for legacy platforms.

Reinstalling drivers and applications

Drivers and applications are software that enable operating systems to communicate with the hardware devices and software in your computer. Devices such as video and sound cards require drivers to function correctly, and enable users to adjust hardware settings.

Device-specific drivers may have to be downloaded and installed separately. Dell Technologies recommends that you download the device drivers for your Dell Technologies computer from Drivers & Downloads.

Applications must be downloaded and installed separately. Dell Technologies recommends that you download the required applications for your Dell Technologies computer from the Dell Download Center.

Displaying drivers and applications on your computer

- 1. Turn on your computer.
- 2. Go to Dell Support Site.
- **3.** In the **Search support** field, enter the Service Tag, Serial Number, Service Request, Model, or Keyword of your computer, and then click **Search**.
 - (i) **NOTE:** If you do not have the Service Tag, Serial Number, Service Request, Model, or Keyword, use the SupportAssist feature to automatically identify your computer. You can also click **Browse all products** to manually browse for your computer.
- 4. Click Drivers & downloads.
- 5. In the **Operating system** drop-down, select the operating system that is installed on your computer to get a list of the drivers and applications available for your computer.

6

Getting help and contacting Dell

Self-help resources

You can get information and help on Dell products and services using these self-help resources:

Table 1. Self-help resources

Self-help resources	Resource location		
Information about Dell products and services	Dell Site		
Tips	·••		
Contact Support	In Windows search, type Contact Support, and press Enter.		
Online help for operating system	Windows Support Site		
	Linux Support Site		
	Windows IoT Enterprise		
Access top solutions, diagnostics, drivers and downloads, and learn more about your computer through videos, manuals, and documents.	Your Dell computer is uniquely identified using a Service Tag or Express Service Code. To view relevant support resources for your Dell computer, enter the Service Tag or Express Service Code at Dell Support Site.		
	For more information about how to find the Service Tag for your computer, see Locate the Service Tag on your computer.		
Dell knowledge base articles	 Go to Dell Support Site. On the menu bar at the top of the Support page, select Support > Support Library. In the Search field on the Support Library page, type the keyword, topic, or model number, and then click or tap the search icon to view the related articles. 		

Contacting Dell

To contact Dell for sales, technical support, or customer service issues, see Dell Support Site.

(i) NOTE: Availability of the services may vary depending on the country or region, and product.

() NOTE: If you do not have an active Internet connection, you can find contact information in your purchase invoice, packing slip, bill, or Dell product catalog.