

Dell ThinOS 10.x 2502, 2505, and 2508

Migration Guide

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.

Chapter 1: Introduction to Dell ThinOS 10.x Migration.....	5
About this guide.....	5
Intended audience.....	5
Overview to ThinOS 10.x migration.....	5
Compatible platforms.....	6
Chapter 2: Choosing the right ThinOS 10.x migration path.....	7
Upgrade devices from ThinOS 9.x to ThinOS 10.x.....	7
Convert devices to ThinOS 10.x.....	7
Understand ThinOS 10.x licensing rules and scenarios.....	7
Chapter 3: Preparing ThinOS 10.x deployment environment.....	9
Downloading ThinOS 10.x packages for deployment.....	9
Download ThinOS firmware, BIOS, and application packages.....	9
Download ThinOS 10.x ISO image.....	10
Prepare a USB drive for ThinOS installation using Dell OS Recovery Tool.....	10
Prepare PXE server setup.....	15
Setting up the PXE server.....	16
File naming convention.....	16
Chapter 4: Upgrading devices to ThinOS 10.x.....	17
Upgrading ThinOS devices using WMS.....	17
Upgrade ThinOS 9.x to ThinOS 10.x using WMS.....	17
Registering device for upgrade.....	18
Upgrading packages for On-premises environment.....	21
Upgrading ThinOS devices using USB.....	23
Upgrade ThinOS from USB drive for Dell platform.....	23
Upgrade ThinOS from USB drive for non-Dell platform.....	25
Upgrading ThinOS devices using PXE	28
Chapter 5: Converting devices to ThinOS 10.x.....	29
Convert Dell Hybrid Client to ThinOS 10.x.....	29
Convert to Dell client devices with Ubuntu 24.04 for Managed Clients.....	30
Convert IGEL OS to ThinOS 10.x.....	31
Register Ubuntu 24.04 for Managed Clients + DCA as Generic Client to WMS.....	32
Register Dell client devices with Ubuntu 24.04 for Managed Clients + DCA as Generic Client to WMS manually.....	32
Register Ubuntu 24.04 for Managed Clients + DCA as Generic Client by using DHCP option tags or DNS SRV records.....	33
Rollback guidance.....	34
ThinOS 10.x upgrade or downgrade using WMS.....	34
Chapter 6: Validating ThinOS 10.x migration success.....	35
Export DHC policies using WMS.....	35

Convert JSON to ThinOS UTC using WMS.....	35
Import UTC file into WMS.....	36
Policy and package setup for ThinOS 10.x conversion.....	36
Migrating ThinOS 9.x policies to ThinOS 10.x using WMS.....	36
Migrating ThinOS 9.x configurations to ThinOS 10.x.....	37
ThinOS 10.x system configuration and group management using WMS	37
ThinOS 10.x configuration grouping using WMS.....	37
System variables.....	38
Chapter 7: Managing BIOS settings for ThinOS devices.....	40
Upgrade BIOS using WMS.....	40
BIOS setting configuration.....	40
BIOS configuration details.....	41
Chapter 8: Removing unused packages and optimizing ThinOS system performance.....	45
Delete ThinOS 10.x application packages using Admin Policy Tool.....	45
Delete ThinOS 10.x application packages using WMS.....	45
Chapter 9: Support Resources.....	47
FAQs.....	47
How do I verify if my device can be converted to ThinOS 10.x?.....	47
How to create and configure DHCP option tags?.....	47
How to create and configure DNS SRV records?.....	48
How to retrieve secure WMS and Group Registration Key?.....	49
Log collection.....	49
Error logs for ThinOS 10.x devices.....	49
Resources and support.....	49
Reference materials and supporting documentation.....	50
Contacting Dell.....	50
Chapter 10: Appendix: Reference and licensing.....	52
Abbreviations.....	52
ThinOS 10.x 2508 application packages.....	53
Returning unused ThinOS subscription licenses	54
Online activation of license key	54
Offline exchange of license key.....	54
ThinOS 10.x subscriptions allocation.....	55

Introduction to Dell ThinOS 10.x Migration

Dell ThinOS 10.x is a secure, deployment-ready operating system that is designed to deliver thin client functionality with minimal resource requirements. It integrates seamlessly with virtual desktop infrastructure (VDI) environments and supports unified communications, authentication, and device monitoring.

During the planning phase of migrating or converting to ThinOS 10.x, the ThinOS 10.x Compatibility Checker runs on non-qualified devices to assess hardware compatibility with ThinOS. It generates a report that identifies any issues, enabling informed decision-making and reducing risk by validating hardware readiness before deployment.

Related Links:

[Reference materials and supporting documentation](#)

Topics:

- [About this guide](#)
- [Intended audience](#)
- [Overview to ThinOS 10.x migration](#)
- [Compatible platforms](#)

About this guide

This guide provides the procedures and tools required to migrate to Dell ThinOS 10.x. It covers upgrade steps from ThinOS 9.x and conversion workflows for IGEL OS, Dell Hybrid Client, and Dell devices running Ubuntu 24.04 for Managed Clients.

Content is organized by user roles, including IT administrators, field engineers, network specialists, and developers. Each section aligns tasks with available Dell tools and platform requirements to support accurate implementation and reduce deployment errors.

This migration guide serves as a critical resource for ensuring a smooth, scalable, and future-ready transition to ThinOS 10.x.

Intended audience

This guide is designed for:

- IT administrators responsible for device migration, OS conversion, endpoint configuration, policy setup, and deployment workflows.
- Support personnel handling device provisioning, troubleshooting, and user assistance during migration.
- Field engineers performing on-site implementation and validation of ThinOS 10.x installations.
- Network specialists managing network connectivity, authentication protocols, and unified communications integration.
- Developers using Dell tools and APIs to configure, extend, or automate ThinOS functionality.

Overview to ThinOS 10.x migration

There are two migration scenarios for transitioning to ThinOS 10.x. Each scenario requires specific roles, tools, and workflows. To support consistent implementation across teams, a persona-based framework is used to map responsibilities and relevant documentation sections to the individuals most involved in each path.

Migration paths

- Upgrade from ThinOS 9.x—Devices running ThinOS 9.x are upgraded using Wyse Management Suite (WMS). This process includes downloading ThinOS 10.x firmware and application packages, applying updates through WMS, and verifying device readiness. For more information, see

- Conversion from other platforms—Supported platforms include Dell Hybrid Client, IGEL OS, and Dell devices running Ubuntu 24.04 for Managed Clients. These require operating system replacement, USB or PXE-based imaging, and registration with WMS for policy configuration and monitoring. For more information, see

The following table outlines the personas that are involved in each scenario, their core responsibilities, and the sections of the guide most relevant to their tasks.

The following table covers the process of upgrading to ThinOS 10.x:

Table 1. Roles and responsibilities for ThinOS 10.x upgrade

Role	Responsibilities	Reference section
IT admin	Plans and performs ThinOS 9.x to 10.x upgrades using WMS	Choosing the right ThinOS 10.x migration path
Field engineer	Performs on-site firmware upgrades and BIOS updates	Preparing ThinOS 10.x deployment environment
Support engineer	Verifies upgrade success and resolves post-upgrade issue	Upgrading devices to ThinOS 10.x
IT admin	Validates post-upgrade configurations and device registration	Validating ThinOS 10.x migration success

The following table covers the process of converting devices from Dell Hybrid Client, IGEL OS, and Dell platforms running Ubuntu 24.04 for Managed Clients to ThinOS 10.x using imaging tools and Wyse Management Suite (WMS):

Table 2. Roles and responsibilities for ThinOS 10.x conversion

Role	Responsibilities	Reference section
Decision maker	Evaluates conversion feasibility and licensing impact	Choosing the right ThinOS 10.x migration path
IT admin	Deploys conversion packages and configures WMS policies.	Upgrading devices to ThinOS 10.x
Field engineer	Converts devices from DHC, IGEL OS, Ubuntu 24.04 for Managed Clients—or reimages using USB—to ThinOS 10.x for consistent client management.	Converting devices to ThinOS 10.x
IT admin	Validates post migration configurations	Validating ThinOS 10.x migration success

Compatible platforms

The Hardware Compatibility List (HCL) identifies supported Dell and non-Dell hardware platforms for ThinOS 10.x and outlines tools that are used to verify compatibility.

ThinOS 10.x runs on validated Dell thin clients and select non-Dell commercial devices that meet minimum hardware and component requirements.

Compatibility is evaluated using the Hardware Compatibility List (HCL) and the ThinOS 10.x Compatibility Checker, which assess whether a device meets deployment requirements.

Platform support details:

- Validated Dell devices—Listed in ThinOS 10.x Hardware Compatibility List. For more information, see *ThinOS 10.x Hardware Compatibility List* document at [Support | Dell](#).
- Dell devices not listed—Validation requests can be submitted through Dell Sales.
- Non-Dell Devices—Use the Compatibility Checker to confirm minimum requirements. For more information, see [Dell ThinOS 10.x Compatibility Checker User Guide](#).

Choosing the right ThinOS 10.x migration path

This chapter guides IT administrators in preparing for ThinOS 10.x deployment, including upgrade and conversion paths, licensing rules, required tools, and key tasks.

- Identifying whether a device should be upgraded or converted.
- Running the ThinOS10.x Compatibility Checker to verify hardware readiness.
- Downloading firmware images, application packages, and conversion tools.
- Setting up Wyse Management Suite (WMS) policies.
- Understanding how licensing applies based on device origin and migration method.

Topics:

- [Upgrade devices from ThinOS 9.x to ThinOS 10.x](#)
- [Convert devices to ThinOS 10.x](#)
- [Understand ThinOS 10.x licensing rules and scenarios](#)

Upgrade devices from ThinOS 9.x to ThinOS 10.x

Upgrade ThinOS 9.x devices to ThinOS 10.x using Wyse Management Suite or USB drive. It includes step-by-step instructions for firmware deployment, license verification, and device registration.

For more information about Upgrade devices from ThinOS 9.x to ThinOS 10.x, see [Upgrading devices to ThinOS 10.x](#).

Convert devices to ThinOS 10.x

Convert eligible devices running Dell Hybrid Client, IGEL OS, or Dell client devices with Ubuntu 24.04 for Managed Clients to ThinOS 10.x. It is recommended that you run the ThinOS 10.x Compatibility Checker on Dell or non-Dell devices to verify eligibility by checking the minimum hardware requirements prior to conversion.

It includes:

- Conversion prerequisites—hardware, firmware, and software requirements.
- WMS policy setup—how to configure and apply conversion policies.
- License handling—steps for managing ThinOS licensing during conversion.
- Registration methods—options for registering converted devices with WMS.

Each conversion path has its own requirements and workflow.

For more information about the eligible Dell and non-Dell devices, see *ThinOS 10.x Hardware Compatibility List* document at [Support | Dell](#).

For more information about conversion scenarios, see [Converting devices to ThinOS 10.x](#).

Understand ThinOS 10.x licensing rules and scenarios

Licensing behavior for ThinOS 10.x devices depends on the method that is used for upgrade or conversion. Administrators must understand how licenses are applied, retained, or required based on the origin of the device and deployment path. Devices upgraded from ThinOS 9.x, converted from Dell Hybrid Client, or reimaged using ISO or USB tools each follow distinct licensing rules. The following overview provides clarity on license retention, expiration, and fallback mechanisms to ensure uninterrupted device functionality and compliance with Dell Technologies licensing policies.

Key licensing scenarios

- **Upgraded ThinOS 9.x Devices (Factory Image or BIOS Key)**—Devices that are upgraded using a factory image or BIOS-injected key do not require a new ThinOS 10.x Activation License. They continue to function using the existing ThinOS 9.x license.
- **Converted Dell Hybrid Client (DHC) Devices**—Devices converted from DHC to ThinOS 10.x retain their DHC license. Upon license expiry, a Dell ThinOS 10.x subscription license for Dell Clients is required for continued functionality.
- **Converted Devices using ISO or USB Imaging**—Convert the devices using USB Imaging method with ThinOS 10.x ISO image:
 - Use the DHC license if available in WMS.
 - Fall back to a ThinOS 10.x Activation License if no DHC license is present.
 - Enter a locked state after 30 days if neither license is available, preventing configuration updates from WMS.

License behavior summary

Table 3. License behavior summary

License Type	Scenario	Post Conversion Behavior	License Expiry	On Expiry
BIOS License	Factory-installed ThinOS 9.x/10.x	No additional license required	Never	N/A
ThinOS 9 Activation	ThinOS 9.x to 10.x upgrade	The license is cached from WMS	Never	N/A
Dell Hybrid Client	DHC to ThinOS 10.x	The license is cached from WMS	Yes (subscription-based)	Device requests renewal from WMS
ThinOS 10 Subscription - Dell Client	Ubuntu or other OS to ThinOS 10.x or USB Imaging for Dell Clients	The license is cached from WMS	Yes (subscription-based)	Device requests renewal from WMS
ThinOS 10 Subscription - Third Party Client for non-Dell Hardware	Ubuntu or other OS to ThinOS 10.x for third-party devices	The license is cached from WMS	Yes (subscription-based)	Device requests renewal from WMS

For more information about allocating ThinOS 10.x licenses to WMS, see [ThinOS 10.x subscription allocation](#).

NOTE: When the ThinOS 10 subscription expires, the system enters a 30-day trial period during which subscription-based features remain available. During this time, a watermark appears on all VDI session windows, and a warning is displayed on the login screen until the license is renewed.

NOTE: The ThinOS 10.x subscription license is not revocable or transferable through WMS.

Preparing ThinOS 10.x deployment environment

This chapter outlines the steps that are required before deploying ThinOS 10.x. It includes downloading the correct firmware, BIOS, ISO, and application packages for upgrades, conversions, and recovery. It also covers how to prepare a USB drive using the Dell OS Recovery Tool, set up a PXE server, and follow proper file naming conventions to ensure a smooth deployment process.

Topics:

- [Downloading ThinOS 10.x packages for deployment](#)
- [Prepare a USB drive for ThinOS installation using Dell OS Recovery Tool](#)
- [Prepare PXE server setup](#)
- [File naming convention](#)

Downloading ThinOS 10.x packages for deployment

Provides an overview of the available ThinOS 10.x 25xx packages that support upgrades, conversions, and recovery options. Describes package titles, file names, and usage scenarios to help you select the correct package for their specific deployment or upgrade path.

Download ThinOS firmware, BIOS, and application packages

Explains how to download ThinOS 10.x firmware, BIOS, and application packages from the Dell Support site. It includes step-by-step instructions to locate and download specific update packages for different upgrade scenarios, supported models, and use cases—such as upgrading from ThinOS 9.x, converting from Dell Hybrid Client, and installing add-on packages like Citrix, VMware, Zoom, and more.

Steps

1. Go to [Support | Dell](#).
2. Click **Browse All Products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **Wyse Software**.
6. Click **Dell ThinOS**.
7. Click **Select This Product**.
8. Click **Drivers & Downloads**.
9. Select the **Operating System** as **ThinOS 10**.
10. Locate the required ThinOS Image entry and click **Download**.

Table 4. Available ThinOS 10.x 25xx package options

Scenario	ThinOS 10 package title	File name
Upgrade from ThinOS 10.x 2502 to ThinOS 10.x 25xx (same version family)	ThinOS 10 25xx Firmware Upgrade Package	RootOS_25xx_10.0xxx_T10.pkg
Convert Dell Hybrid Client or Ubuntu 24.04 for Managed Clients to ThinOS 10	Dell Hybrid Client/Ubuntu 24.04 for Managed Clients to ThinOS 10 25xx Conversion Package	DellHybridClient_Ubuntu_To_ThinOS10_conversion_25xx_10.xxx.tar.gz

Table 4. Available ThinOS 10.x 25xx package options (continued)

Scenario	ThinOS 10 package title	File name
Download Dell Recovery Image	ThinOS 10 25xx Offline USB Installer Package	ThinOS10_25xx_0127.iso
Upgrade from ThinOS 9.5.3102 or later to ThinOS 10.x 25xx	ThinOS 9.5.3102 or later to ThinOS 10 25xx Upgrade Package	Root_25xx.10_0xxx_signed.pkg

11. To use ThinOS packages, select the package and click **Download**.
For more information, see [ThinOS 10.x 25xx application packages](#).
12. To install the latest BIOS package, select the BIOS package <version>— entry corresponding to your thin client model, and click **Download**.
For information about BIOS installation, see [BIOS Installation](#).



Download ThinOS 10.x ISO image

Explains how to use the ThinOS 10.x ISO image to install the operating system on supported devices through a USB drive using the Dell OS Recovery Tool. The ISO image is downloaded as a .zip file and must be extracted before use.

About this task

To download the ISO image, do the following:

Steps

1. Go to [Support | Dell](#).
2. Click **Browse All Products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **Wyse Software**.
6. Click **Dell ThinOS**.
7. Click **Select This Product**.
8. Click **Drivers & Downloads**.
9. Select the **Operating System** as **ThinOS 10**.
10. Download the ThinOS 10.x latest version.
 **NOTE:** The ISO image is provided in a ZIP file. You must extract the ISO file before using it with the Dell OS Recovery Tool.
11. Download recovery image for non-Dell platform.
 **NOTE:** To obtain the Dell recovery image, go to [Support | Dell](#), enter the Service Tag or product identifier, and search for the latest ThinOS 10.x recovery image. Use the same image for recovery/offline USB imaging.

Prepare a USB drive for ThinOS installation using Dell OS Recovery Tool

Explains how to use a USB drive and the Dell OS Recovery Tool to install ThinOS 10.x image on supported devices.

Steps

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**.

- After the installation is complete, open Dell OS Recovery Tool.
- Select **SWITCH TO ADVANCED RECOVERY** displayed at the bottom of the tool.

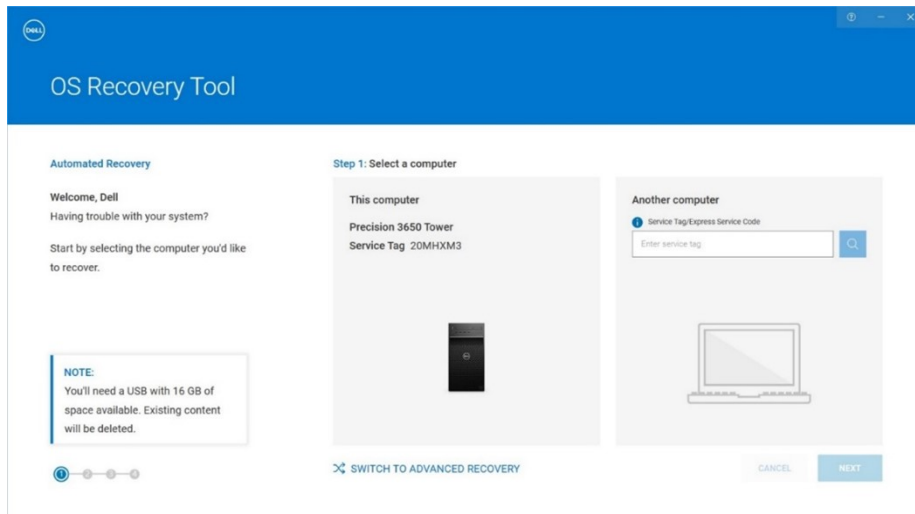


Figure 1. Dell OS Recovery Tool

- In **Select an OS image**, browse to the ISO file that you downloaded on the device, and click **NEXT**.

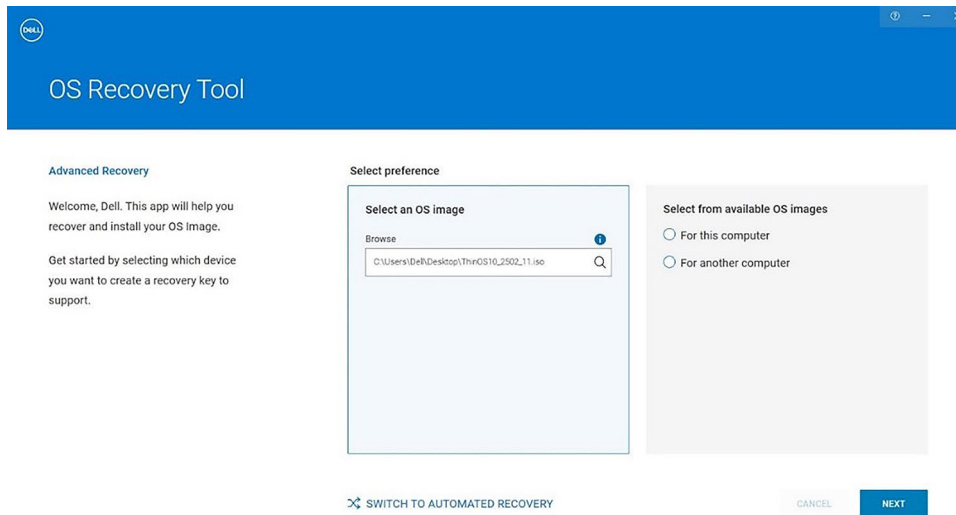


Figure 2. Upload the ISO file

NOTE: Do not select from the pre-populated OS list. Doing so disables the ISO upload option.

NOTE: Certain special USB drives do not support ThinOS ISO image by default. You can change the **Partition Style** and reconfigure the operating system. You can either select the partition as GPT or MBR and proceed further.

- Select the USB drive that you want to format from the **USB drive** dropdown.
- Check the **I understand that the selected drive will be reformatted and existing data will be deleted** box.
- Click **BURN OS**.

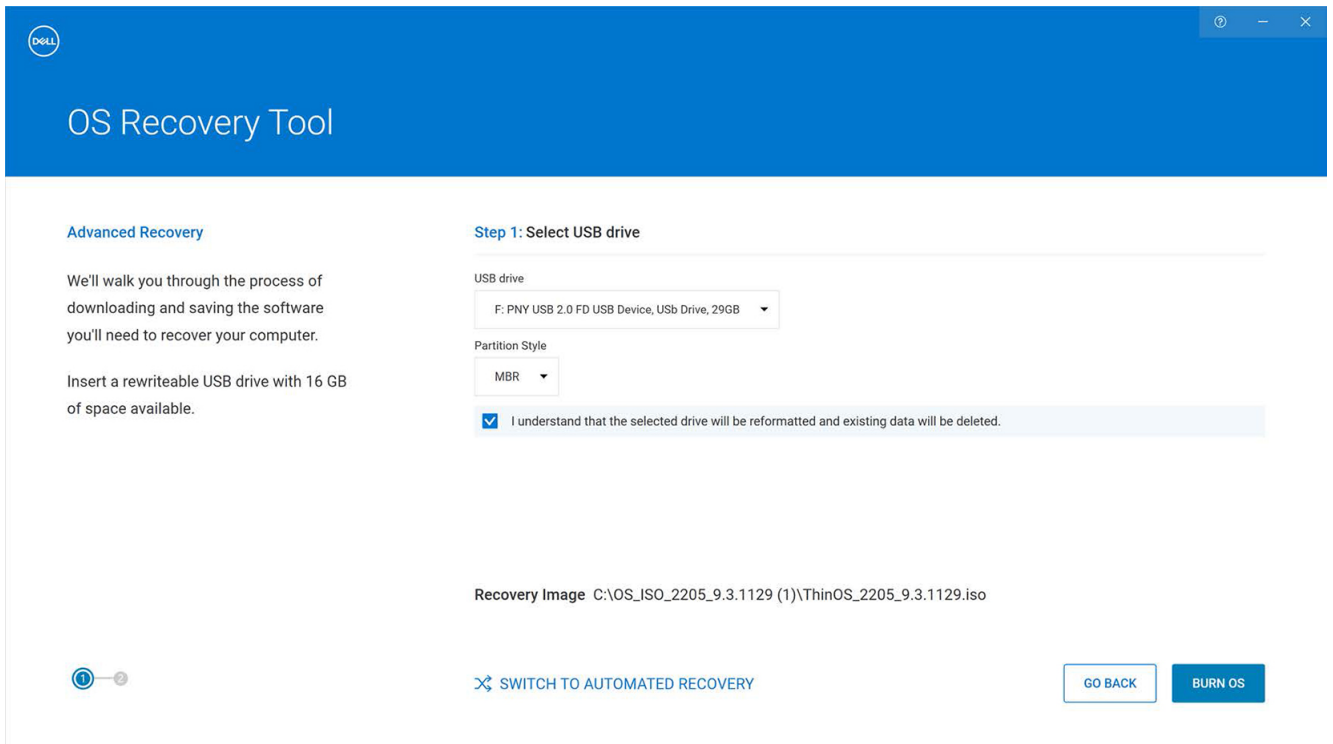


Figure 3. Burn OS

10. Remove the USB drive and connect it to the device that is powered off, on which you plan to install ThinOS. After connecting the USB drive, turn on the device.

NOTE: Once the burn OS process is completed, the build is stored in the USB drive. After the USB drive is removed, Dell OS Recovery Tool goes back to the screen that is displayed in Step 5.

11. Power on the device and during bootup, click **F2**. The device BIOS page opens.
12. If prompted for a BIOS password, enter the default password: **Fireport** (case-sensitive), and click **OK**.

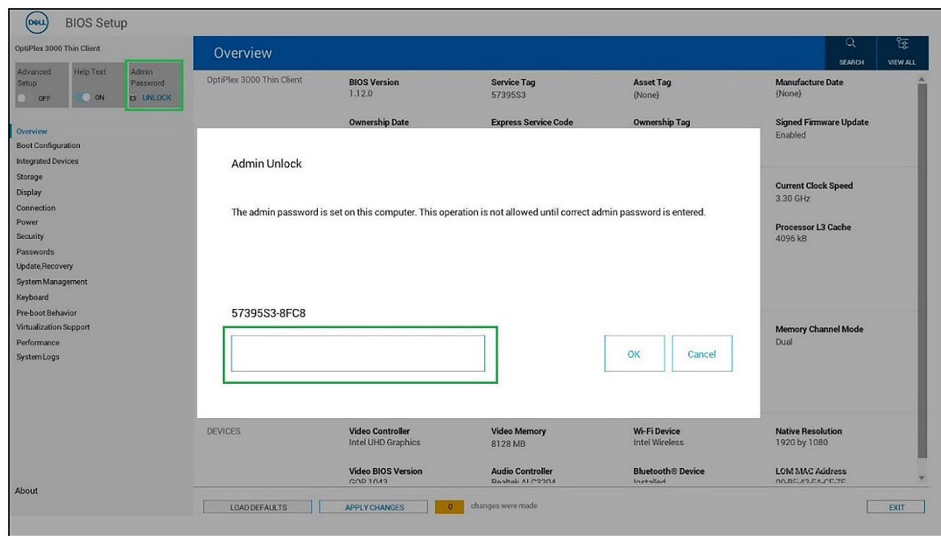


Figure 4. Unlock BIOS Screen

NOTE: The password is case sensitive and after unlocking successfully, the **Admin Unlock** dialog box closes.

13. Go to the **Integrated Devices** section in **BIOS Setup**.
14. Select the **Enable USB Boot Support** checkbox.

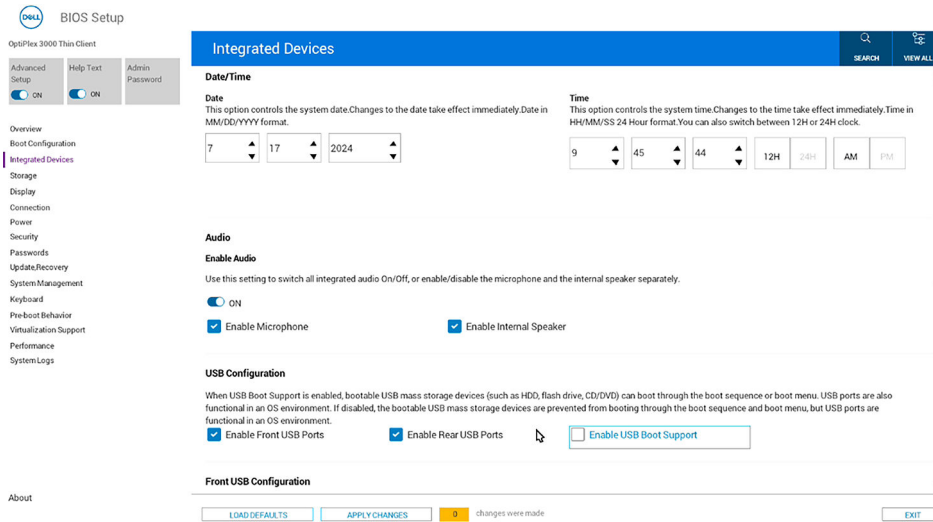


Figure 5. Enable USB Boot Support

15. Go to the **Security** section in **BIOS Setup**.
16. Enable the **Start Data Wipe** setting under **Data Wipe on Next Boot**.

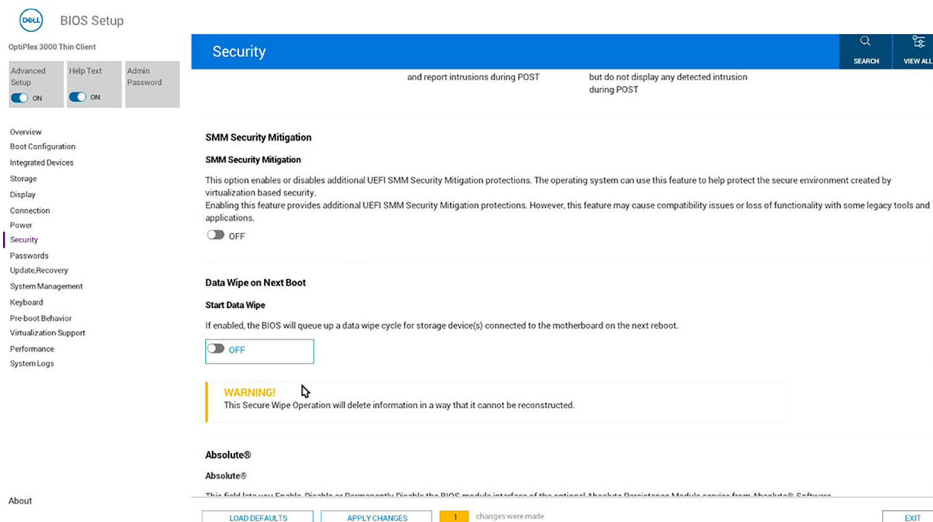


Figure 6. Data Wipe Screen

A **Data Wipe** dialog box is displayed to confirm the change.

17. Click **OK** to continue the data wipe process.

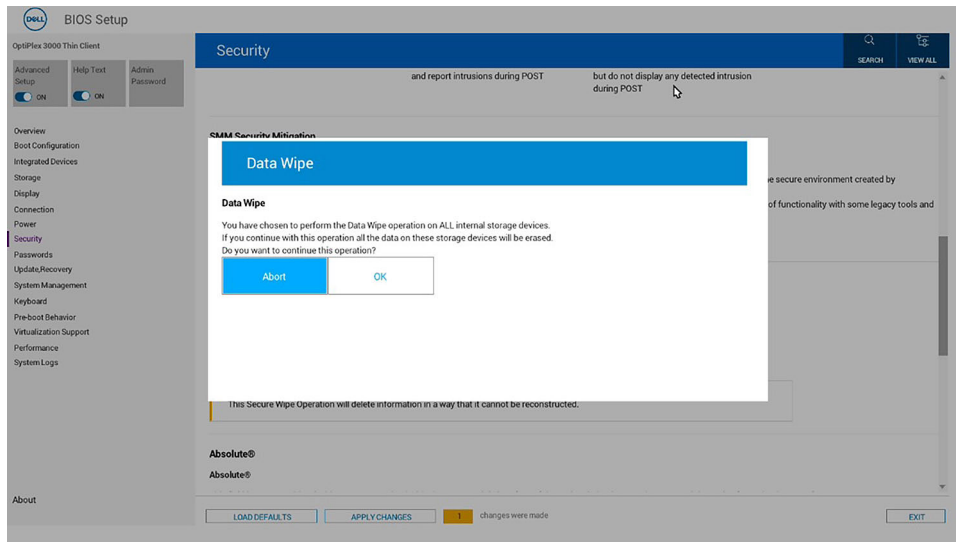


Figure 7. Data Wipe Screen (Select OK)

NOTE: You are prompted again to cancel or continue the process.

18. Click **No**.
19. Scroll down and enable the **Clear** setting in the **Security** section to clear the user information. A **Clear TPM** dialog box is displayed to confirm the change.

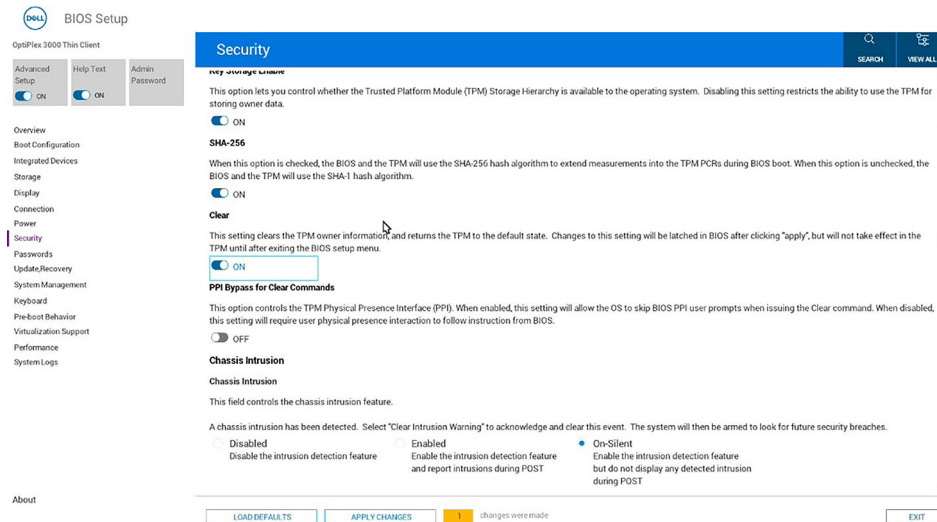


Figure 8. Clear TPM

20. Click **Yes**.
21. Exit BIOS Settings. If prompted, select **Yes** to save the changes. The **Dell Security Manager** dialog box is displayed.

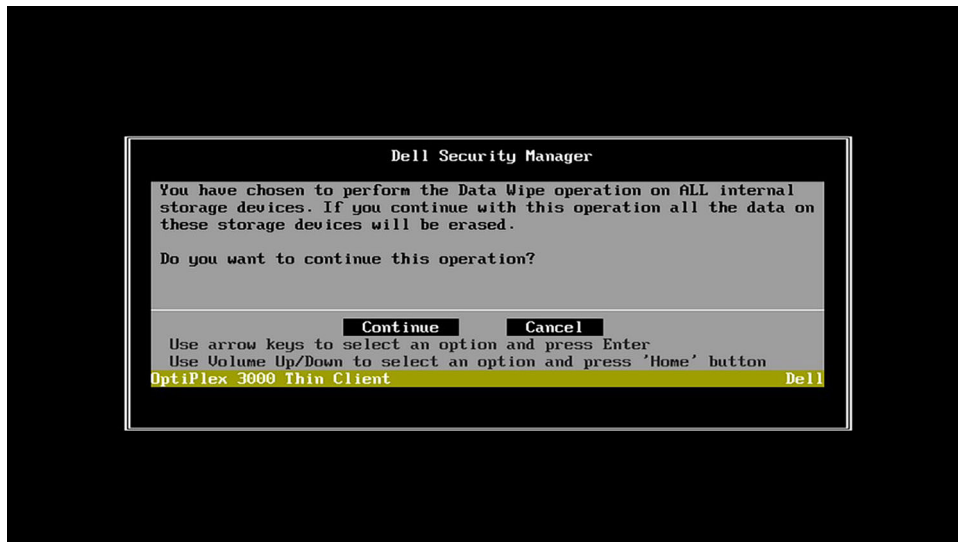


Figure 9. Dell Security Manager Screen (Select continue)

22. Click **Continue**.
23. Click **Erase**.
The data wipe process is complete.
24. Click **OK**.

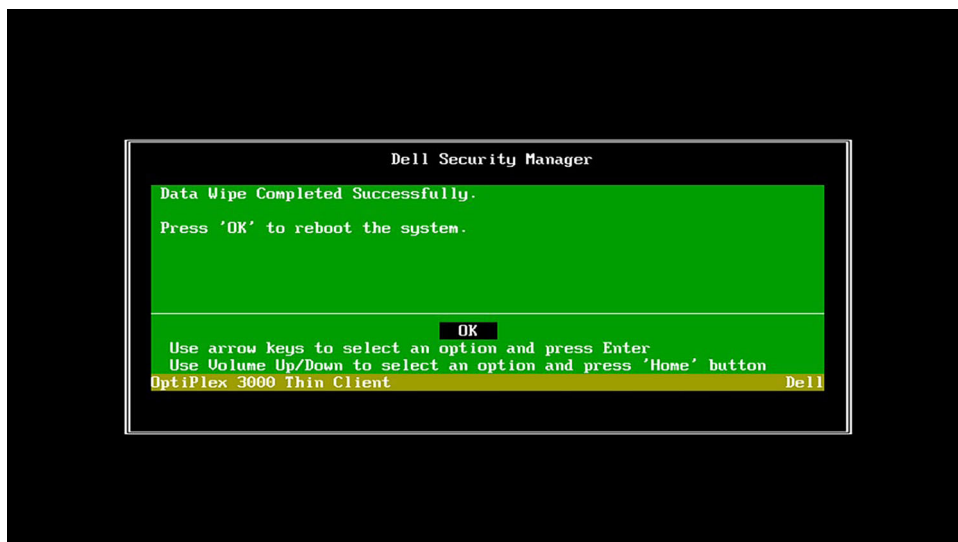


Figure 10. Dell Security Manager Screen (Select OK)

The device starts rebooting.

Prepare PXE server setup

Describes how to set up a PXE server for ThinOS 10.x upgrades by configuring the PXE server, DHCP server, and TFTP client within the same subnet to ensure seamless communication and reliable boot operations.

- PXE Server
- DHCP Server
- TFTP Client

Keeping all components in the same subnet ensures smooth communication and a reliable PXE boot process.

Setting up the PXE server

Describes how to configure a PXE server on Ubuntu 20.04 or later for upgrading ThinOS devices to ThinOS 10.x, including TFTP setup, DHCP options, and required packages.

Prerequisites

- Use a system running Ubuntu 20.04 or later (virtual or physical) as the PXE server.
- Assign a static IP address to the PXE server.
- Ensure that this IP is outside the DHCP scope to avoid IP conflicts during PXE boot.

Steps

1. To set up the PXE server, install the necessary packages using the following commands:

```
$ sudo apt-get update
```

```
$ sudo apt-get install tftpd-hpa
```

```
$ sudo apt-get install apache2
```

2. To setup TFTP, do the following:
 - a. Download the `pxe_secure_boot.zip` file and the ThinOS ISO file to your **Downloads** directory.
 - b. Download the ThinOS ISO in the same **Downloads** directory on your device.
 - c. Run the following commands to configure the TFTP server:

```
$ unzip pxe_secure_boot.zip
```

```
$ cd pxe_secure_boot
```

```
$ chmod +x pxe_setup.sh
```

```
$ sudo ./pxe_setup.sh <path to iso>
```


3. To setup the DHCP server, configure the following DHCP options:
 - **066–Boot Server Host Name:** Specify the IP address of the boot server (for example: 100.106.90.101).
 - **067–Bootfile Name:** Set the boot file name to **bootx64.efi**.These configurations direct the client to the appropriate boot server and boot file during the PXE boot process.

File naming convention

ThinOS application packages, ThinOS firmware, BIOS packages, and other files can be published from the Wyse Management Suite server.

The file names must adhere to the following character rules:

- Uppercase letters (A–Z)
- Lowercase letters (a–z)
- Numeric characters (0–9)
- Special characters—period (.), hyphen-minus (-), and underscores (_)

 **NOTE:** Using any other characters in the file name results in installation failure.

Upgrading devices to ThinOS 10.x

This chapter provides step-by-step instructions for upgrading ThinOS 9.x devices to ThinOS 10.x using WMS, USB, or PXE, including registration and license validation.

To upgrade the ThinOS devices from older versions to the latest version, do any of the following:

- Upgrade ThinOS 9.x to ThinOS 10.x using WMS.
 - Upgrade ThinOS from USB drive using Dell OS Recovery Tool.
- NOTE:** Downgrading from version 10.x to 9.x is not supported. To install an earlier version, you must manually download the 9.x package and install it.

Topics:

- [Upgrading ThinOS devices using WMS](#)
- [Upgrading ThinOS devices using USB](#)
- [Upgrading ThinOS devices using PXE](#)

Upgrading ThinOS devices using WMS

Explains how to upgrade ThinOS devices to the latest release using Wyse Management Suite (WMS). It covers upgrading ThinOS 9.x to 10.x, registering devices for upgrade through DHCP/DNS or Wyse Device Agent, and configuring package updates in both cloud and on-premises environments.

Upgrade ThinOS 9.x to ThinOS 10.x using WMS

Upgrade ThinOS 9.x to ThinOS 10.x using WMS, which allows you to schedule, manage, and monitor the upgrade process across multiple devices.

Steps

1. Log in to **Wyse Management Suite** as administrator.
2. Go to the **Groups & Configs** page, and select a group.
3. From the **Edit Policies** drop-down menu, select **ThinOS 9.x**.
The **Configuration Control | ThinOS** window is displayed.
4. Go to **Advanced**.
5. In the **Firmware** field, select **OS Firmware Updates**.
6. Click **Browse** to browse and upload the firmware.
The EULA and vendor details are displayed.
7. Verify the vendor names and license agreement and then click **Accept** to upload the package.
8. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the `Root_25xx.10_00xx_signed.pkg` package from the local repository.
9. Click **Save & Publish**.
An alert window is displayed.
10. Click **Save** to save the changes.
11. On the device, click **Download** button to check if the package is getting downloaded.
The thin client begins downloading the firmware, and a notification appears on the screen.
12. Click **Update Now**.
The device downloads the firmware and once the upgrade is successful, it reboots to the desktop screen.
13. Click the **System Information** icon to view the system information window.
14. Go to the **License** tab and verify that the license information is displayed.
15. Confirm that the **License Type** shows as **BIOS License** or **ThinOS Activation License**.

The firmware version is upgraded successfully.

NOTE: In cloud environments, ThinOS 10.x application, BIOS, and firmware packages are available in the Operator Cloud and Tenant Cloud.

NOTE: Existing policy configurations for ThinOS 9.x can remain active until new configurations are created for the ThinOS 10.x group.

Registering device for upgrade

Explains how to register ThinOS devices to the WMS using auto-discovery methods or manual registration. Devices can automatically discover the WMS server through IPv4/IPv6 DHCP options and DNS configuration, or you can manually register them using the Wyse Device Agent (WDA).

Register devices to WMS

ThinOS Automated Deployment enables streamlined provisioning of thin client devices by allowing them to automatically receive configurations and software updates upon connecting to the network. This process is managed through centralized tools such as WMS or designated file servers. WMS facilitates the automated deployment of ThinOS devices by defining and applying key environmental settings, ensuring consistent and efficient device configuration across the enterprise.

NOTE: DHCP and DNS SRV configurations for WMS can only function if your device is not already registered.

NOTE: If both WMS server and secure WMS server are set, the secure WMS server takes priority. If both a unique group token key and a secure unique group token key are set, the secure token key takes priority.

Table 5. DHCP and DNS configuration for WMS

Environment	Definition	IPv4 DHCP User-Defined Option	IPv6 DHCP User-Defined Option	DNS Resource Record
WMS Server	Specifies the WMS server.	Option 165 (String)	Option 16500 (String)	_WMS_MGMT (SRV)
WMS Server	Specifies the secure WMS server.	Option 201 (String)	Option 20100 (String)	_WMS_MGMTV2 (Text)
WMS MQTT Server (optional)	Specifies the MQTT server.	Option 166 (String)	N/A	_WMS_MQTT (SRV)
WMS CA Validation	Specifies whether the CA validation is required when you import certificates into your WMS server.	Option 167 (String)	Option 16700 (String)	_WMS_CAVALIDATION (Text)
WMS Group Token	Specifies a unique key that is used by WMS to associate the ThinOS client to the device group Policy. From Wyse Management Suite 3.5, the group tokens are case-sensitive. The DHCP and DNS values also have to be configured with case-sensitive values.	Option 199 (String)	Option 19900 (String)	_WMS_GROUPTOKEN (Text)
WMS Group Token	Specifies a secure unique key that is used by WMS to associate the ThinOS client to the device group Policy.	Option 202 (String)	Option 20200 (String)	_WMS_GROUPTOKENV2 (Text)

NOTE: It is recommended that you do not define more than one type of management or configuration delivery method.

NOTE: If the Group Token parameter is not specified, the device is moved to the unmanaged group or quarantine group. This is applicable for On-premises WMS.

For more information about creating and configuring DHCP option tags, see [How to create and configure DHCP option tags?](#).

Register ThinOS 10.x devices with DHCP IPv4 and IPv6 option tags

Explains how to register ThinOS 10.x devices to WMS with IPv4 and IPv6 DHCP option tags for server, MQTT, certificate validation, and group registration. Register the devices by using the following DHCP option tags:

Table 6. Registering device with IPv4 DHCP option tags

Option Tag for IPv4	Option Tag for IPv6	Description
<ul style="list-style-type: none"> Name—WMS Data Type—String Code—201 Description—WMS Server FQDN 	<ul style="list-style-type: none"> Name—WMS Data Type—String Code—16500 Description—WMS Server FQDN 	<p>This tag directs the device to the URL of the WMS server. For example, <code>wmsserver.acme.com</code>, where <code>wmsserver.acme.com</code> is the fully qualified domain name of the server hosting the WMS.</p> <p>NOTE: HTTPS:// is not required in the WMS URL.</p>
<ul style="list-style-type: none"> Name—WMS Data Type—String Code—201 Description—Secure WMS Server 	<ul style="list-style-type: none"> Name—WMS Data Type—String Code—20100 Description—Secure WMS Server 	<p>This tag directs the device to the WMS server.</p>
<ul style="list-style-type: none"> Name—MQTT Data Type—String Code—166 Description—MQTT Server 	Not applicable	<p>This tag directs the device to the WMS Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the WMS server. For example, <code>wmsservername.domain.com:1883</code>. WDA automatically fetches the MQTT details when devices check in for the first time.</p> <p>NOTE: MQTT is optional for WMS 5.0 or later versions.</p>
<ul style="list-style-type: none"> Name—CA Validation Data Type—String Code—167 Description—Certificate Authority Validation 	<ul style="list-style-type: none"> Name—CA Validation Data Type—String Code—16700 Description—Certificate Authority Validation 	<ul style="list-style-type: none"> You can enable or disable the CA validation option if you are registering your devices with WMS on private cloud. Enter True, if you have imported the SSL certificates from a well-known authority for https communication between the client and the WMS server. Enter False, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the WMS server. <p>NOTE: CA Validation is optional for WMS 5.0 or later versions. However, it is recommended to configure this option tag.</p>
<ul style="list-style-type: none"> Name—Group Registration Key Data Type—String Code—199 Description—Group Registration Key 	<ul style="list-style-type: none"> Name—Group Registration Key Data Type—String Code—19900 Description—Group Registration Key 	<p>The tag directs the device to retrieve the Group Registration Key for WMS. For example, in <code>SCDA-DTOS10SalesGroup</code>, the second part of the Group Registration Key must be 8-31 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character. However, special characters such as <code>\</code> (backslash), <code>"</code> (double quotes), <code>'</code> (single quote) are not allowed. The Group Registration Key is case-sensitive.</p> <p>NOTE: The Group Token is optional when using WMS 5.0 on a premises-based server. However, due to a known issue, if the Group Token is not provided, the device may not be moved to an unmanaged group. Therefore, it is recommended to configure the Group Token to ensure proper device registration.</p>

Table 6. Registering device with IPv4 DHCP option tags (continued)

Option Tag for IPv4	Option Tag for IPv6	Description
<ul style="list-style-type: none"> Name—Group Registration Key Data Type—String Code—202 Description—Secure Group Registration Key 	<ul style="list-style-type: none"> Name—Group Registration Key Data Type—String Code—20200 Description—Secure Group Registration Key 	The tag directs the device to retrieve the secure Group Registration Key for WMS.

NOTE:

If only IPv6 is available in your network and IPv4 is absent, the system requires approximately 5 minutes for the IPv4 DHCP to time out. After this timeout, the system automatically discovers WMS using IPv6 DHCP. To avoid this delay during each reboot, ensure that IPv4 is disabled in your WMS policy.

Configure devices with DNS SRV record

Describes WMS Server, MQTT, Group Token, and CA Validation User-Defined Options defined using a DNS service.

Table 7. Configure devices with DNS SRV record

Option tag	Description
WMS server (_WMS_MGMT, Type SRV, Protocol _tcp, Port number 443)	This record directs the device to the WMS URL. For example, <code>wmsserver.acme.com</code> , where <code>wmsserver.acme.com</code> is the qualified domain name of the server. NOTE: There is a known issue that <code>https://</code> is required in the WMS server URL. If you do not use <code>https://</code> , the device cannot automatically check in to WMS.
WMS server (_WMS_MGMTV2, Type Text)	This record directs the device to a secure WMS server.
(Optional) WMS MQTT Server	This record directs the device to the WMS Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the WMS server. For example, <code>wmsservername.domain.com:1883</code> . NOTE: MQTT is optional for WMS 5.0 or later versions.
WMS Group Token (_WMS_GROUPTOKEN, Type Text)	This record is required to register the ThinOS device with WMS on public or private cloud. NOTE: Group Token is case-sensitive. However, it is optional for WMS 5.0 on prem-server.
WMS Group Token (_WMS_GROUPTOKENV2, Type Text)	This record directs the device to secure Group Registration Key for WMS.
WMS CA Validation (_WMS_CAVALIDATION, Type Text)	<ul style="list-style-type: none"> You can enable or disable the CA validation option if you are registering your devices with WMS on private cloud. By default, the CA validation is enabled in the public cloud. You can also disable the CA validation in the public cloud. Enter True, if you have imported the SSL certificates from a well-known authority for https communication between the client and the WMS server. Enter False, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the WMS server. NOTE: CA Validation is optional for WMS 5.0 or later versions.

For more information about creating and configuring DNS SRV records, see [How to create and configure DNS SRV records?](#).


For more information about retrieving the secure WMS server and secure Group Registration key, see [How to retrieve secure WMS and Group Registration Key?](#).

Register ThinOS devices using Wyse Device Agent

Configure the WDA agent directly from the ThinOS. This configuration must be done individually on each device.


Steps

1. On the ThinOS device, access the central configuration settings:
 - **Modern Mode**—From the desktop menu, click **Settings > Central Configuration**.
 - **Classic Mode**—From the desktop menu, click **System Setup > Central Configuration**.The **Central Configuration** dialog box is displayed.

 **NOTE:** Privilege must be set to **High** or Admin Mode must be activated to access to the ThinOS Central Configuration menu.
2. Select the **Enable WMS Advanced Settings** checkbox.
3. In the **WMS server** field, enter the WMS URL in the format `https://server.domain`.

This value represents the WMS server from which ThinOS clients are managed and the device configurations are obtained over SSL.
4. In the **Group Registration Key** field, enter the group registration key as configured by your WMS administrator for your group. To verify the setup, click **Validate Key**.

If the key is not validated, verify the group key and WMS server URL that you have provided. Ensure that the network is not blocking the default ports, which are 443 and 1883.

 **NOTE:** If the Group Token parameter is not specified, the device is moved to the unmanaged group or quarantine group.
5. Enable or disable **CA Validation** based on your license type. For public cloud, select the checkbox. For private cloud, select the **Enable CA Validation** checkbox if you have imported certificates from a well-known certificate authority into your WMS server.


To enable the CA validation option in the private cloud, you must install the same self-signed certificate on the ThinOS device. If you have not installed the self-signed certificate in the ThinOS device, do not select the **Enable CA Validation** checkbox. You can install the certificate to the device by using WMS after registration, and then enable the CA validation option.
6. Validate the newly added devices enrollment in WMS, to become manageable. You can enable the **Enrollment Validation** option to allow administrators to control both manual and automatic registration of thin clients to a group.

When the **Enrollment Validation** option is enabled, the manual or auto discovered devices are in the Enrollment Validation Pending state on the **Devices** page. The tenant can select a single device or multiple devices on the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see the **Enrollment Validation** section in *Wyse Management Suite 5.0 Administrator's guide* at [Support | Dell](#).
7. Click **Save**.

The device checks in to the WMS, and the policy settings are applied.

Upgrading packages for On-premises environment

Explains how to upgrade ThinOS 10.x application, BIOS, and firmware packages available in the public cloud, including Operator Cloud and Tenant Cloud, to keep devices secure, updated, and properly managed.

 **NOTE:** The operator can upload the package from the operator account, and it is visible to all the tenants. Tenants cannot delete or modify these files.


- For On-premises environment, use any of the following methods:
 - [Upload the packages using Group & Configs](#)
 - [Upload the package using Apps & Data](#)
 - [Upload the package using local/remote repository](#)

Upload the package using Groups & Configs

Step-by-step instructions to upload and deploy ThinOS 10.x firmware, BIOS, and application packages using Groups & Configs in WMS.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 10.x**.
The **Configuration Control | ThinOS 10.x** window is displayed.
3. From the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**.
5. Click any of the following:
 - **OS Firmware Updates**
 - **BIOS Firmware Updates**
 - **Application Package Updates**

 **NOTE:** If you cannot locate the **Firmware** option under the **Standard** tab, use the **Advanced** tab.
6. Click **Browse**, and select the ThinOS 10.x package to upload and deploy.

Upload the package using Apps & Data

Step-by-step instructions to upload ThinOS 10.x firmware, BIOS, and application packages using the Apps & Data tab in WMS.

Steps

1. Log in to Wyse Management Suite using your tenant credentials.
2. In the **Apps & Data** tab, go to **OS Image Repository**.
3. Click **ThinOS 10.x**.
4. Click any of the following:
 - Click **Add Firmware file** for adding the firmware package.
 - Click **Add BIOS file** for adding BIOS package.
 - Click **Add package file** for adding application package.The **Add Package** screen is displayed.
5. Click **Browse**, and navigate to the stored location where the file is saved.
 - If the EULA is embedded in the package, the EULA details of the package and the name of the vendors are displayed. You can select the vendor names to read the license agreement of each vendor. Click **Accept** to upload the package. You can select the **Do not show this again** if you do not want to see the EULA details of the same vendor again. You must accept the license agreement of the packages individually. The package is not uploaded if you click **Decline**.
 - If the EULA is not embedded in the package, go to step 6.
6. Click **Upload**.

Upload the package using local/remote repository

Upload ThinOS 10.x packages by copying them to a local or remote repository in WMS for automatic synchronization.

ThinOS 10.x firmware, application, and BIOS packages can be directly copied to the:

- Local repository—C:\WMS\LocalRepo\repository\thinOSConfigFiles.

Or

- Remote repository—C:\WMS\RemoteRepo\repository\thinOSConfigFiles.

The packages are synchronized to WMS and appear under the ThinOS 10.x operating system repository user interface.

Upgrading ThinOS devices using USB

Explains how to upgrade ThinOS devices to the latest release using a USB drive. It provides procedures for both Dell and non-Dell platforms with the Dell OS Recovery Tool.

Upgrade ThinOS from USB drive for Dell platform

Explains how to upgrade ThinOS on Dell platforms using a USB drive created with the Dell OS Recovery Tool. Describes how to boot from the USB, install ThinOS, complete the out-of-box experience (OOBE), accept the license agreement, select language, and log in to the ThinOS 10.x desktop.

Steps

1. Connect the USB drive to the device.
2. Turn on the device.
3. Press F12 at boot up until you see the Dell logo and **Preparing one-time boot menu...** displayed at the top, right corner. The BIOS boot menu opens.
4. In the boot menu, select the USB drive from the **UEFI Boot Devices** list.

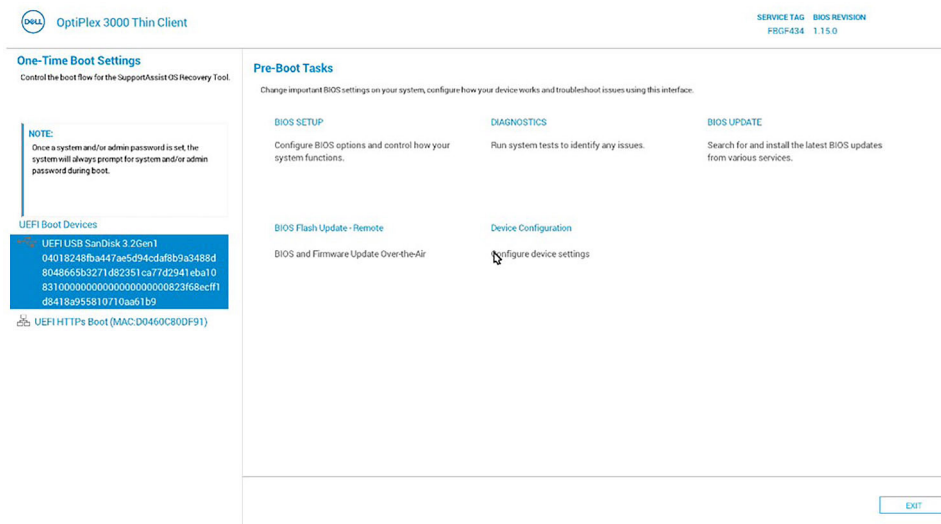


Figure 11. UEFI Boot Devices USB (Select)

5. Exit **BIOS**.
Your device automatically reboots, and installation begins. After installation, the OOBE screen is displayed.

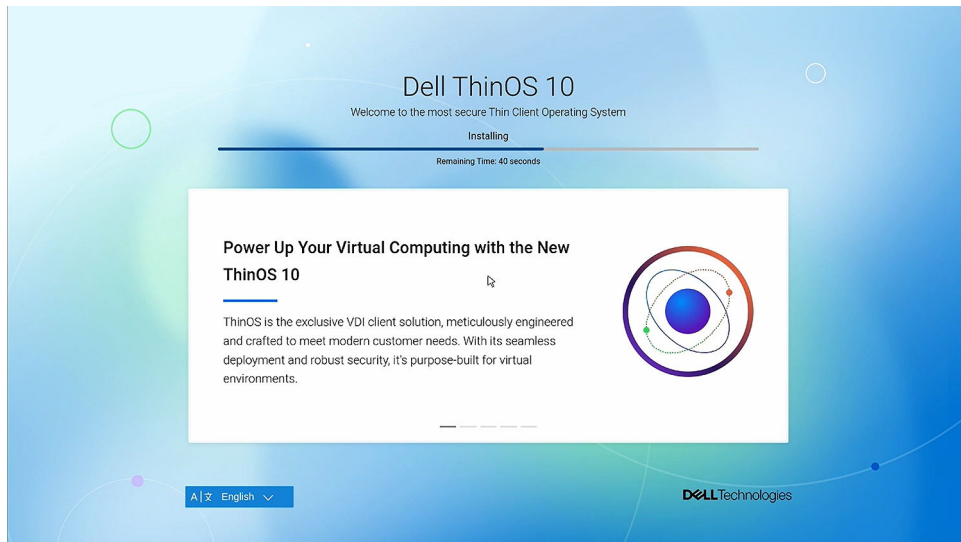


Figure 12. Installation Screen

6. Click the arrow button to go to the **Review License Agreement** page.

NOTE: If a network cable is connected, the device directly goes to the Review License Agreement page after obtaining your IP address. If WMS discovery is configured, then the device skips the OOBE screen.

7. In the **Review License Agreement** page, select **Accept All**.

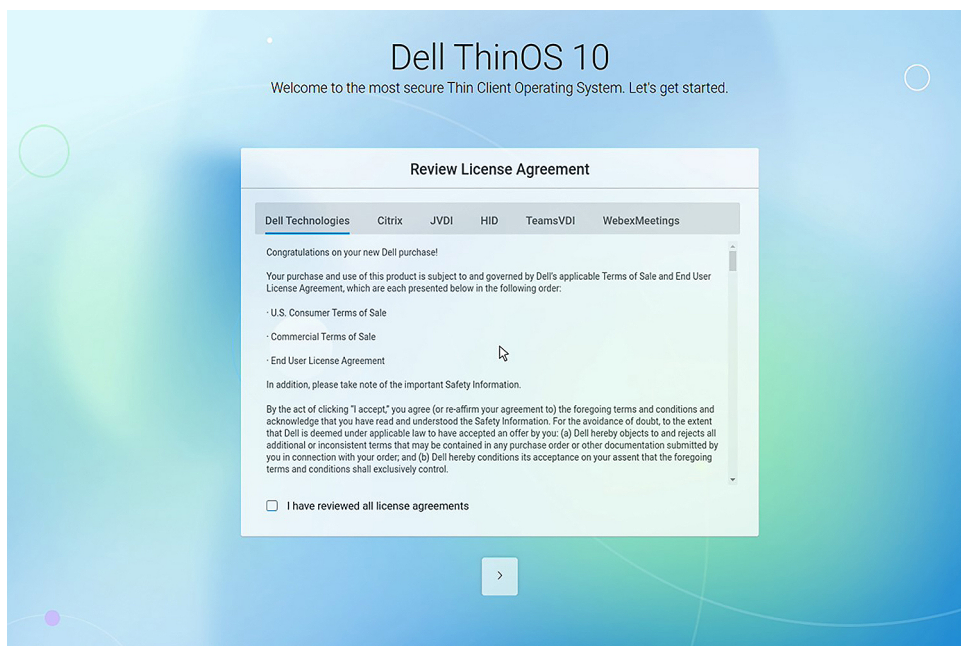


Figure 13. OOBE Screen

8. Click the arrow button to go to the **Select Your Language** page. Select the language that you want to use with ThinOS 10.

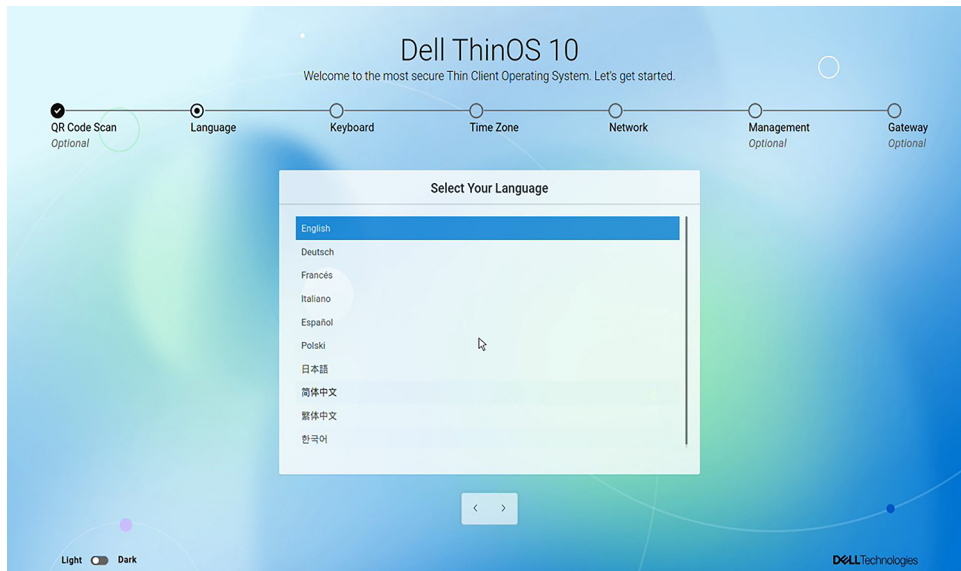


Figure 14. OOB Screen (Language Selection)

9. Press the Ctrl + Esc key combination to log in to your ThinOS 10 device. The device logs in to your desktop screen.

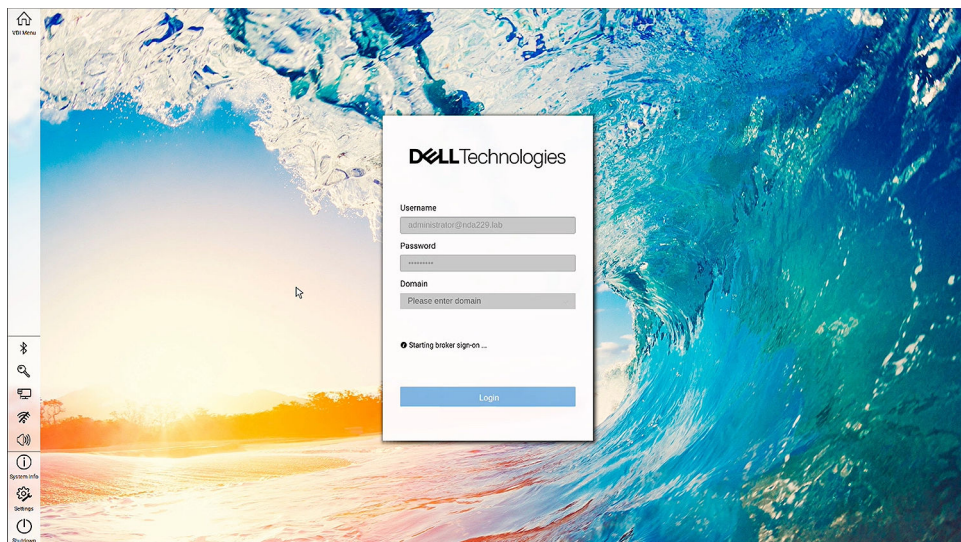


Figure 15. Desktop Screen

Upgrade ThinOS from USB drive for non-Dell platform

Explains how to upgrade ThinOS on non-Dell platforms using a USB drive created with the Dell OS Recovery Tool. Describes how to boot from the USB, install ThinOS, complete the out-of-box experience (OOBE), accept the license agreement, select language, and log in to the ThinOS 10.x desktop.

Steps

1. Connect the USB drive to the device.
2. Turn on the device.
3. Press F10 or F12 at boot up until you see the Dell logo and **Preparing one-time boot menu...** displayed at the top, right corner. The BIOS boot menu opens.
4. In the boot menu, select the USB drive from the **UEFI Boot Devices** list.

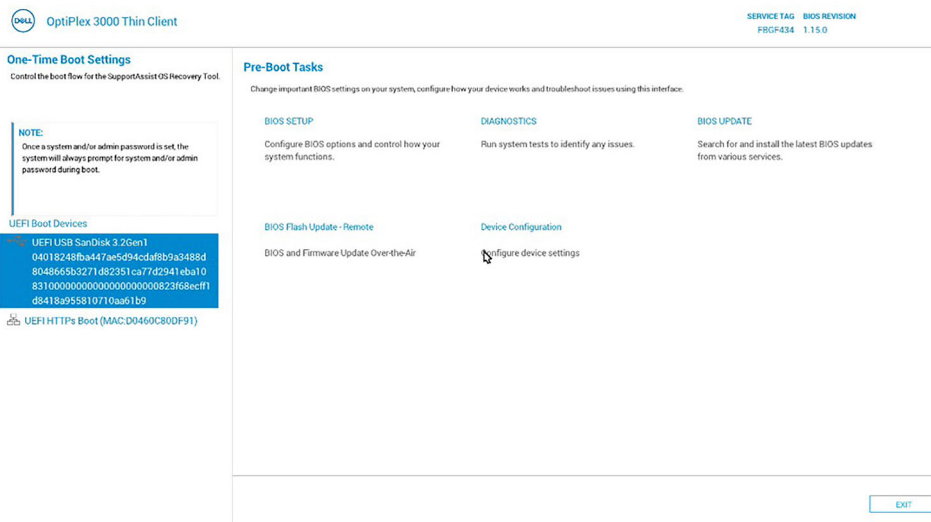


Figure 16. UEFI Boot Devices USB (Select)

5. Exit **BIOS**.
Your device automatically reboots, and installation begins. After installation, the OOB screen is displayed.

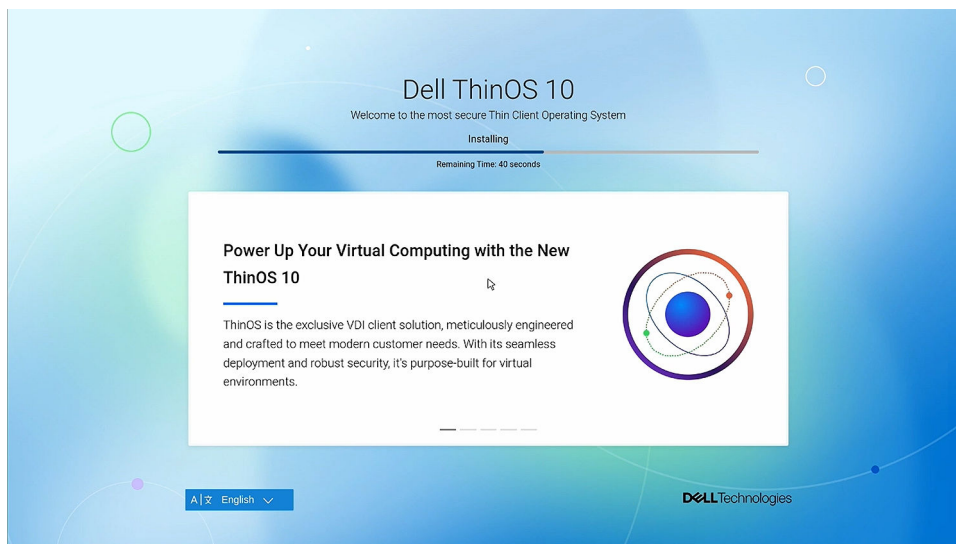


Figure 17. Installation Screen

6. Click the arrow button to go to the **Review License Agreement** page.
 - NOTE:** If a network cable is connected, the device directly goes to the Review License Agreement page after obtaining your IP address. If WMS discovery is configured, then the device skips the OOB screen.
7. In the **Review License Agreement** page, select **Accept All**.

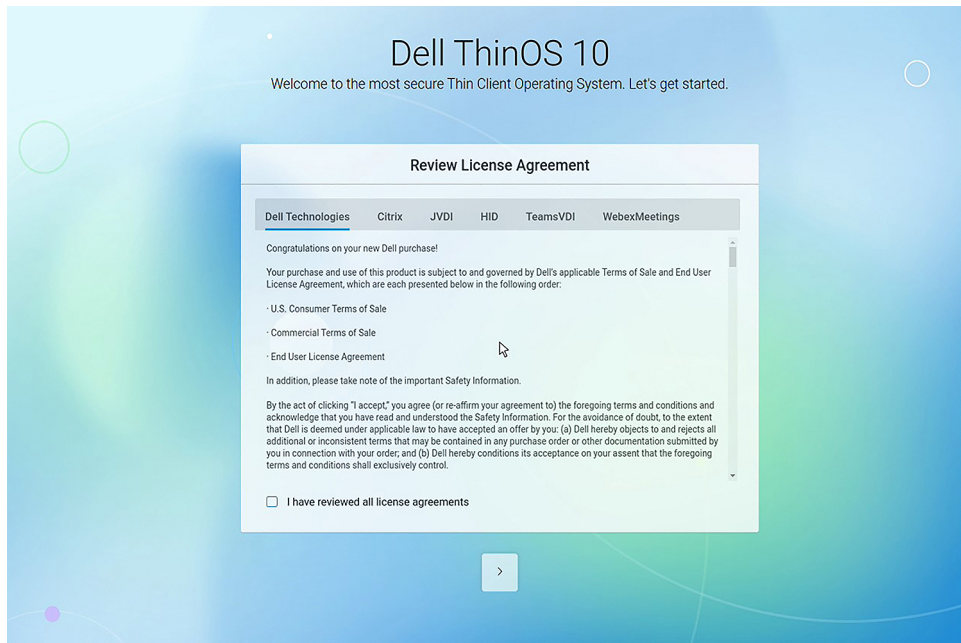


Figure 18. OOB Screen

8. Click the arrow button to go to the **Select Your Language** page. Select the language that you want to use with ThinOS 10.

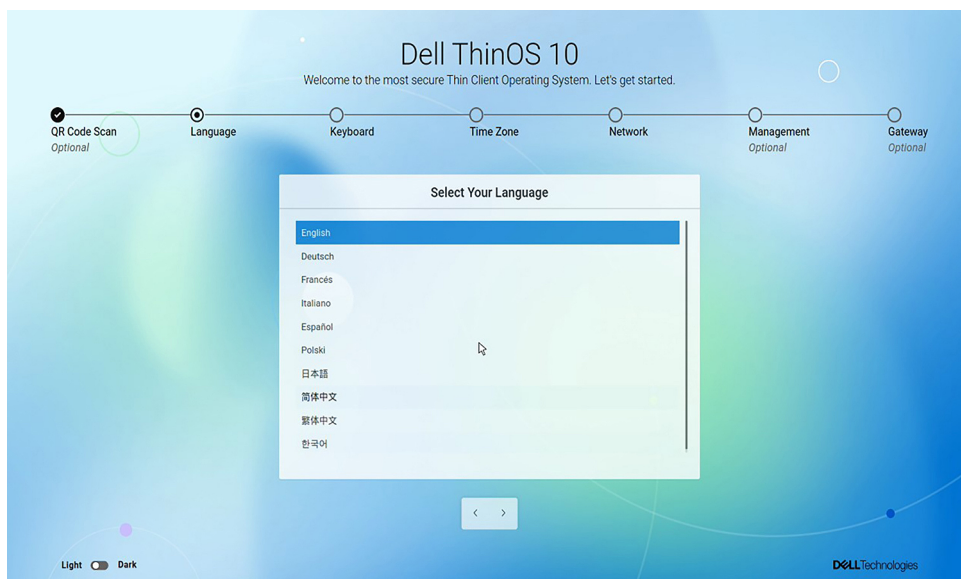


Figure 19. OOB Screen (Language Selection)

9. Press the Ctrl + Esc key combination to log in to your ThinOS 10 device. The device logs in to your desktop screen.

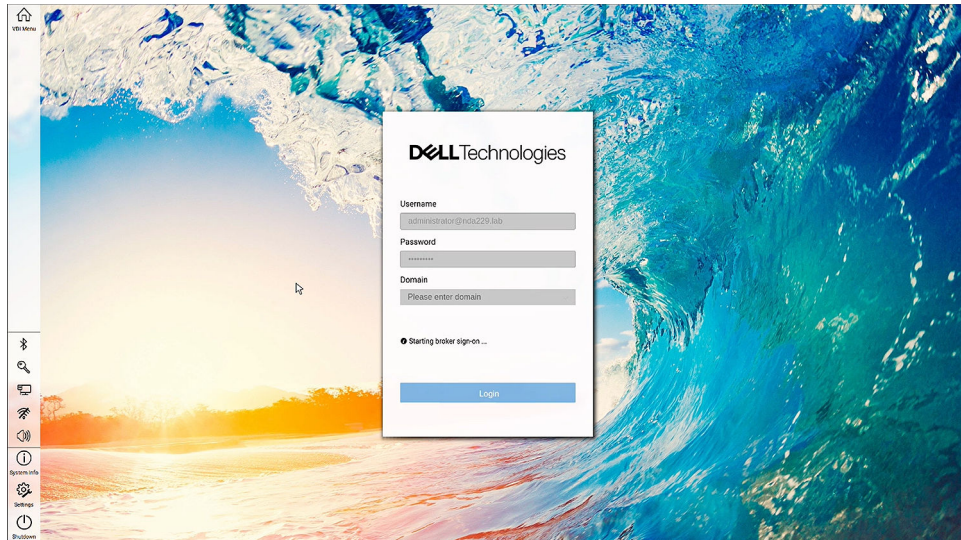


Figure 20. Desktop Screen

Upgrading ThinOS devices using PXE

Explains how to upgrade ThinOS 10.x devices using PXE by setting up the PXE infrastructure with DHCP and TFTP, enable PXE Boot support in WMS, uploading the PXE boot package, and configure DHCP tags to support automated zero-touch installation.

Steps

1. Log in to **WMS console**.
2. Go to **Groups & Configs > BIOS**, and enable **PXE Boot Support** option.
3. Restart the device to apply the changes.
4. Go to the **Groups & Configs** page, and select a group.
5. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
The **Configuration Control | ThinOS** window is displayed.
6. In the left pane, click **Standard**.
7. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.
i **NOTE:** If you cannot locate the **Firmware** option under the **Standard** tab, use the **Advanced** tab.
8. Click Browse and select the **PXEBoot<version>.pkg** to upload.
9. After successful installation, restart the device to apply the PXE Boot entries.
i **NOTE:** For automatic registration, ensure the DHCP tags (167, 165, 199) are configured on the DHCP server. The device automatically starts the OS installation with zero-touch behavior, requiring no additional manual intervention.

Converting devices to ThinOS 10.x

This chapter describes the conversion process from IGEL OS, Dell Hybrid Client, and Ubuntu 24.04 for Managed Clients to ThinOS 10.x, including prerequisites, tools, and rollback options.

NOTE: Run the ThinOS 10.x Compatibility Checker to ensure that the device meets the minimum hardware requirements. For more information, see [Dell ThinOS 10.x Compatibility Checker User Guide](#).

Topics:

- [Convert Dell Hybrid Client to ThinOS 10.x](#)
- [Convert to Dell client devices with Ubuntu 24.04 for Managed Clients](#)
- [Convert IGEL OS to ThinOS 10.x](#)
- [Register Ubuntu 24.04 for Managed Clients + DCA as Generic Client to WMS](#)
- [Rollback guidance](#)

Convert Dell Hybrid Client to ThinOS 10.x

Convert Dell Hybrid Client devices to ThinOS 10.x, deploy the DHC conversion package using WMS. This process helps you reimage supported devices, apply the necessary policies, and deploy ThinOS through a scheduled job, making the transition smooth and retaining existing licenses when applicable.

Prerequisites

- WMS version 5.0 or later must be used to convert Dell Hybrid Client to ThinOS 10.x.
- Ensure that you have connected the device to the external power source using the power adapter.
- Ensure that you have enough ThinOS 10.x Activation devices licenses on WMS.
- If Dell Hybrid Client devices have a valid, unexpired Dell Hybrid Client activation license, ThinOS 10.x continues to use the Dell Hybrid Client license after conversion, and the device does not use a ThinOS 10.x license.
- Create a group in WMS with a group token.
- The Dell Hybrid Client devices must be registered to WMS.
- Ensure to download the Dell Hybrid Client to DHC_Ubuntu_To_ThinOS10_conversion_25xx_10.00xx.tar package conversion image.

Steps

1. Log in to **Wyse Management Suite** as administrator.
2. Copy DHC_Ubuntu_To_ThinOS10_conversion_25xx_10.0xxx.tar to C:\WMS\LocalRepo\repository\hybridClientApps or do the following:
 - a. Go to **Apps & Data**.
 - b. Go to **App Inventory**, and select **Dell Hybrid Client**.
 - c. Select **Add Package file**.
The **Add Package** window is displayed.
 - d. Click **Browse**, and select the DHC_Ubuntu_To_ThinOS10_conversion_25xx_10.0xxx.tar package.
 - e. Click **Upload**.
3. Go to **Apps & Data > App Policies > Dell Hybrid Client**, and click **Add Advanced Policy**.
4. Go to the **Add Standard App Policy** section and enter the **policy name** of your choice.
5. Go to the **Group Section > Default Device Policy Group**, and select your group.
6. Go to the **Task** section, and select **Install Application** from the drop-down list.
7. Go to the **Application** section > **Add App**, and select the DHC_Ubuntu_To_ThinOS10_conversion_25xx_10.0xxx.tar package from the drop-down list.
8. Click **Save**.
An **Alert** window is displayed.

9. In the dialog window, click **Yes** to schedule a job.
 10. Select **Immediately** in the **Run** drop-down menu on the **App Policy Job** window, and click **Preview**.
 11. Click **Schedule** to initiate the conversion.
After the conversion is scheduled, the ThinOS 10.x image is downloaded and installed on the Dell Hybrid Client device. Upon completion, the device restarts automatically.
 - NOTE:** After conversion, ThinOS is restored to its factory default state. The ThinOS 10.x device is automatically registered to WMS under the same group.
 - NOTE:** If a valid Dell Hybrid Client (DHC) activation license is still active, ThinOS 10.x continues to search for it. If no DHC license is found, the device uses the available ThinOS 10.x activation license.
 - NOTE:** If no DHC or ThinOS 10.x activation license is available, the device continues to work for 30 days. After 30 days, no configurations can be pushed from WMS.
- A **Notification Update** window is displayed on the devices.
12. Click **Update Now** to upgrade the build immediately, or wait 5 minutes for the automatic update.
Once the update completes, the device reboots to the desktop screen.

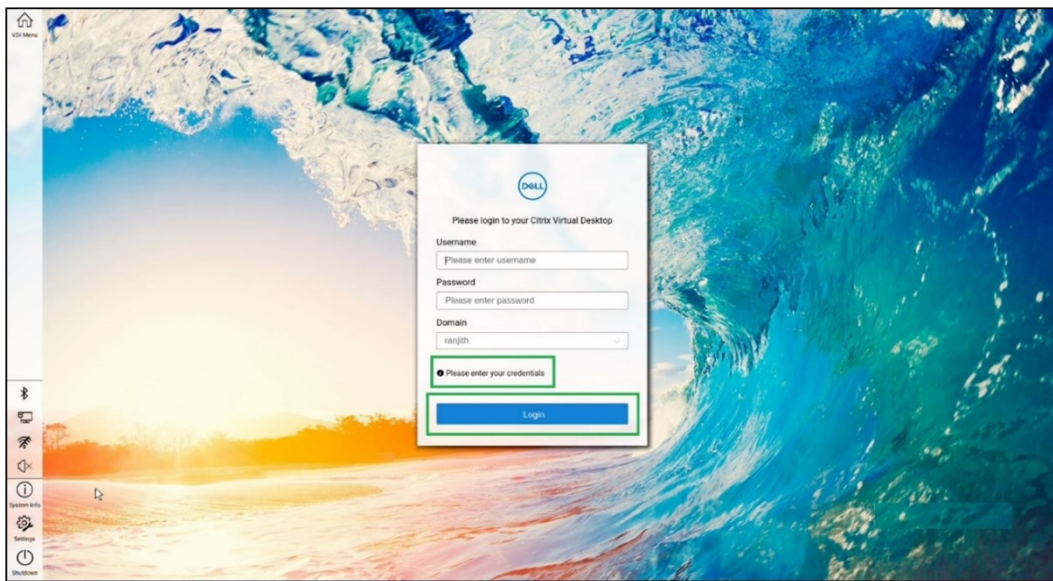


Figure 21. Desktop Screen

The Desktop screen is displayed.

Convert to Dell client devices with Ubuntu 24.04 for Managed Clients

Convert systems with Ubuntu 24.04 for Managed Clients to ThinOS 10.x, use WMS along with the Dell client devices with Ubuntu 24.04 for Managed Clients conversion package. This process allows you to reimage supported devices, apply the necessary policies, and seamlessly transition them to ThinOS for centralized management.

Prerequisites

- WMS version 5.0 or later is required to convert to ThinOS 10.x.
- Ensure that you have connected the device to the external power source using the power adapter.
- Ensure that you have enough ThinOS 10.x Subscription device licenses on WMS.
- Create a group in WMS with a group token.
- The number of ThinOS 10.x Subscription licenses in WMS must be greater than the number of Ubuntu devices to create the Advanced Policy for conversion.
- The Ubuntu devices must be registered to WMS as generic clients. For details on how to register the generic client to WMS, see [Register Dell client devices with Ubuntu 24.04 for Managed Clients + DCA as Generic Client to WMS manually](#).

- Ensure that you have downloaded the `DHC_Ubuntu_To_ThinOS10_conversion_25xx_10.0xxx.tar` conversion image.

If your device is running with the latest Ubuntu 24.04 for Managed Clients operating system, ensure that the relevant DCA-Enabler is installed on the device. For more information about compatible Dell and non-Dell platforms, see *ThinOS 10.x Hardware Compatibility List* document at [Support | Dell](#).

NOTE: The device must have a factory-installed Ubuntu operating system. Manually installed operating system for Dell Devices with Ubuntu 24.04 for Managed Clients are not eligible for conversion to ThinOS 10.x.

Steps

1. Log in to **Wyse Management Suite** as administrator.
2. Go to **Apps & Data > App Inventory > Generic Client**, and click **Add Package file**.
3. Upload the Conversion Installer file `DHC_Ubuntu_To_ThinOS10_conversion_25xx_10.0xxx.tar`.
4. Go to **Apps & Data > App Policies > Generic Client**, and click **Add Advanced Policy**.
5. Enter the policy name, select the group in which the Ubuntu for managed clients has been registered, and select **Generic Client** as **OS** type.
6. Click **Add app** and select the previously uploaded ThinOS image file from the drop-down menu.
7. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
8. Select the platforms to convert from the **Platform Filter** drop-down menu.
9. Click **Save**.
10. In the next window, click **Yes** to schedule a job.
11. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.
12. Click **Schedule**.

The Conversion Installer file downloads and installs first followed by the ThinOS image on the Ubuntu device. After installation, the device restarts automatically.

NOTE: After you register the converted ThinOS device to WMS, the ThinOS activation devices license is used automatically.

NOTE: If a valid Dell Hybrid Client (DHC) activation license is still active, ThinOS 10.x continues to search for it. If no DHC license is found, the device uses the available ThinOS 10.x activation license.

NOTE: After conversion, ThinOS is in the factory default status. ThinOS must be registered to WMS manually or using DHCP/DNS discovery.

NOTE: If the conversion fails, you can see the error log table below and reschedule the job. Go to **Jobs > Schedule APP Policy** to reschedule the job. If the conversion continues to fail, it is recommended you install the ISO image.

If there is a `/usr/dtos` folder in your Ubuntu device, you can use the command `cat /var/log/dtos_dca_installer.log` to get the error log.

If there is no `/usr/dtos` folder in your Ubuntu device, go to the **WMS Server Jobs** page to check the error messages. For more information about the error logs, see [Error Log table](#).

Convert IGEL OS to ThinOS 10.x

ThinOS 10.x 2508 provides a seamless conversion path for IGEL OS versions 11 and 12, allowing these endpoints to be converted to ThinOS 10.x clients. To convert an IGEL device to ThinOS 10.x, begin by registering the device with the **Universal Management Suite** (UMS). Use the **Scan for Devices** feature, which automatically detects IGEL devices that are located within the same subnet as the UMS server or within a specified IP range. It is recommended to run the ThinOS 10.x Compatibility Checker before converting an IGEL device. Intel x86 or x64 configurations are supported for conversion.

Prerequisites

- Ensure that the device has a minimum of 4 GB RAM and 32 GB storage before initiating the IGEL to ThinOS 10.x conversion.
- Ensure that you register an IGEL device with the Universal Management Suite (UMS) using the **Scan for Devices** feature or you can register the device using a **One-Time Password** (OTP) generated from the UMS console. For more information, see [Registering IGEL OS devices on the UMS server](#).

- Ensure that you have downloaded the IGEL conversion .zip package from the **BETA** folder, and extract the required files on your device: `IGEL_UMS_To_ThinOS10_conversion.tar.bz2` and `IGEL_UMS_To_ThinOS10_conversion.inf`.

Steps

1. Launch the UMS console and go to **Server > Files**.
2. Right-click **Files** and select **New Directory** to create a folder for conversion files, or choose **New File** to upload the conversion package directly.
3. Browse and upload both conversion files:
 - `IGEL_UMS_To_ThinOS10_conversion.tar.bz2`
 - `IGEL_UMS_To_ThinOS10_conversion.inf`
4. After uploading, verify that both files `IGEL_UMS_To_ThinOS10_conversion.tar.bz2` and `IGEL_UMS_To_ThinOS10_conversion.inf` are listed under the UMS file server.
5. To configure the custom partition, go to **UMS Web App**, and register the device.
6. In the **UMS Web App**, click **Edit Configuration** for the target IGEL device.
7. Go to **System > System Customization > Custom Partition > Partition** to configure custom partitions that are required for deploying the IGEL conversion package.
8. Enable the **Partition** option.
9. Specify the **Size** in GB using the **G** suffix. For example: 2G for 2 GB.
10. Enter a **Name** for the custom partition, which acts as in **Mount Point Name** for the custom part.
11. Enable **Automatic Update**.
12. Enter the **URL** as the **UMS File Server URL** followed by the `.inf` file name. For example: Enter the complete path of the `.inf` file saved on the device.
13. Enter the **Username** and **Password** credentials.
14. In the **Initial Action** field, specify the script path as: `/bin/sh /<mountpoint name configured in partition section>/custompart-dtos10.sh`.
15. Click **Save and Close**.
After closing, a prompt appears asking whether to apply the configuration **now** or **on reboot**.
16. Select **Now** to apply the changes immediately.
This applies the configuration and reboots the device automatically to install ThinOS 10.x.

Register Ubuntu 24.04 for Managed Clients + DCA as Generic Client to WMS

This chapter outlines how to register Ubuntu 24.04 with DCA as a generic client to WMS, either manually, through DHCP option tags, or using DNS SRV records.

Register Dell client devices with Ubuntu 24.04 for Managed Clients + DCA as Generic Client to WMS manually

Explains how to register Dell client devices on Ubuntu 24.04 with DCA enabler as generic clients to WMS using group token and server details.

Prerequisites

- Create a group in WMS with a group token.
- The device must be preinstalled with DCA enabler version 2.1.0-271 or later.

Steps

1. Open DCA Enabler.
2. Enter the WMS Server and Group Token.
3. Enable or disable CA Validation based on your WMS server license type.

4. Click **Register**.

The device attempts to register with the WMS server, and after registration, the device is listed as **Type = Generic Client**.

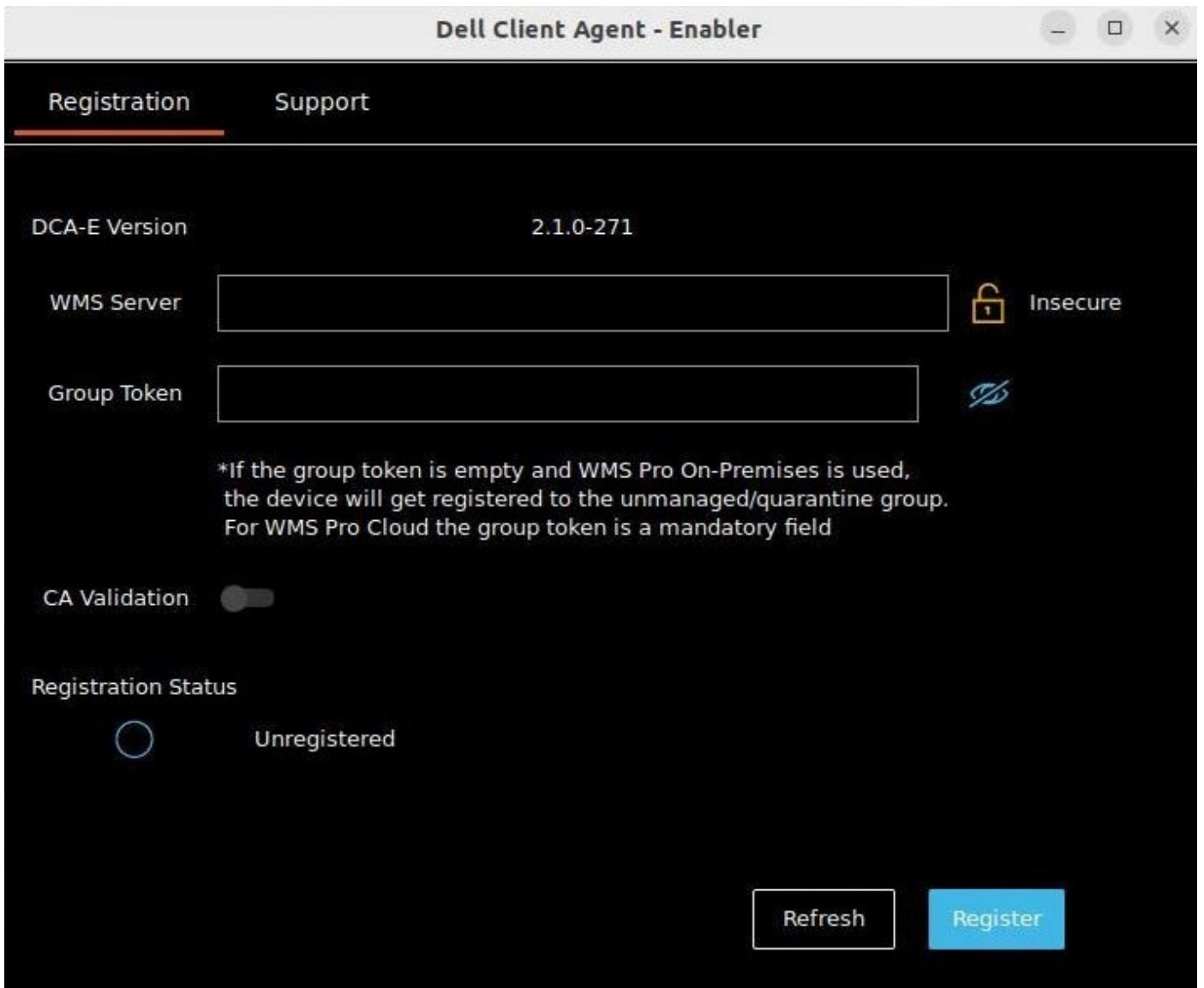


Figure 22. Dell Client Agent - Enabler

Register Ubuntu 24.04 for Managed Clients + DCA as Generic Client by using DHCP option tags or DNS SRV records

Describes how to register Dell devices with Ubuntu 24.04 as generic clients to WMS using DHCP option tags or DNS SRV records, requiring DCA-Enabler 2.1.0-271 or later.

- Ensure that DCA-Enabler 2.1.0-271 or later versions are installed on Dell devices with Ubuntu 24.04 for Managed Clients.
- Create a group in WMS with a group token.

The process to register Ubuntu devices by using DHCP option tags or DNS SRV records is the same as registering ThinOS by using DHCP option tags or DNS SRV records. See [WMS Automation using DHCP and DNS Auto Discovery](#) section.

NOTE: Registering Ubuntu devices as generic clients by using DHCP option tags or DNS SRV records takes about 2 to 3 minutes.

Rollback guidance

Provides rollback guidance for ThinOS 10.x, explaining how to remotely upgrade or downgrade between supported versions using Wyse Management Suite (WMS), with automatic package compatibility and minimal manual effort.

ThinOS 10.x upgrade or downgrade using WMS

ThinOS 10.x (version 2508 and later) supports seamless upgrade and downgrade between ThinOS 10 N and N+1 versions using Wyse Management Suite (WMS). This capability enables remote management, automatic rollback, and configuration alignment without manual intervention.

The following are the key features:

- **Remote upgrade or downgrade initiation**—IT Administrators can initiate ThinOS 10.x upgrades or downgrades remotely using the Wyse Management Suite (WMS) console, streamlining deployment and minimizing endpoint downtime.
- **Add-on package compatibility**—During the upgrade or downgrade process, existing add-on packages are either retained or automatically updated to maintain compatibility with the target ThinOS version.
- **Automatic configuration updates**—WMS automatically updates endpoint configurations to match the upgraded or downgraded ThinOS version, ensuring consistent user experience and system behavior.
- **Automatic rollback on failure**—If an upgrade or downgrade fails, ThinOS automatically reverts to the last known working version to prevent service disruption and maintain endpoint stability.
- **Failure logging and troubleshooting**—The IT Administrators can access the detailed endpoint logs to support debugging and troubleshooting, enabling quick resolution of upgrade issues.
- **Signing certificate tolerance**—ThinOS upgrades and downgrades between N and N+1 versions are not impacted by changes in signing certificates, ensuring a smooth transition.
- **Certificate retrieval from WMS**—If a signing certificate mismatch occurs, the client fetches the correct certificate from WMS to complete the upgrade successfully.

Validating ThinOS 10.x migration success

This chapter describes how to validate ThinOS 10.x migration success by converting and importing policies, verifying configurations, and optimizing system grouping.

Topics:

- [Export DHC policies using WMS](#)
- [Policy and package setup for ThinOS 10.x conversion](#)
- [Migrating ThinOS 9.x policies to ThinOS 10.x using WMS](#)
- [Migrating ThinOS 9.x configurations to ThinOS 10.x](#)
- [ThinOS 10.x system configuration and group management using WMS](#)

Export DHC policies using WMS


The **DHC to T10 Configuration Migration Tool** enables IT Administrators to convert existing DHC policy files into ThinOS 10-compatible policy formats, allowing for streamlined migration and deployment of policies within ThinOS environments. This chapter explains how to migrate existing DHC policies in WMS to a ThinOS 10.x-compatible format using the **DHC to T10 Configuration Migration Tool**, and re-import them for deployment.

Prerequisites

Ensure the following:

- **DHCThinOS10ConfigTool** is installed locally.
- You must first export an existing DHC policy from WMS before using the **DHCThinOS10ConfigTool**.
- Exported policies are available in `.json` format.
- Administrative privileges on both WMS and local device.

Steps

1. Log in to WMS as an administrator.
 2. Go to **Groups & Configs > Configure DHC Policies**.
 3. Click **Export Policies**.
The **Export Policies** window is displayed.
 4. In **Specific Device Type Policies** dropdown menu, select **Dell Hybrid Client**.
 5. Click **Yes** to confirm.
A `.json` file is downloaded containing the current DHC configuration.
-  **NOTE:** Only a subset of DHC policies are supported in ThinOS 10. Unsupported settings are excluded during migration, and the tool generates a list of policies that could not be converted.

Convert JSON to ThinOS UTC using WMS

You can convert `.json` to ThinOS 10.x UTC using WMS.

Steps

1. Open the **DHCThinOS10ConfigTool** on the device.
2. Click **Upload DHC Configuration**.
3. Browse and select the downloaded `.json` file.
4. Once the file is uploaded, click **Save & Export**.
A `.utc` file compatible with ThinOS 10.x is generated and downloaded on the device.

Import UTC file into WMS

You can import **.utc** file into WMS using the WMS console and deploy it to DHC devices.

Steps

1. Log in to **WMS Console**.
2. Go to **Groups & Configs > Import Policies**.
The **Import Polices Wizard** window is displayed.
3. Go to **From and export file** option, and click **Browse**.
4. Select the downloaded **ThinOS 10.x .utc** file, and click **Next**.
The converted ThinOS 10.x policies are successfully imported into WMS and ready for deployment to DHC devices.

NOTE: Ensure that all policy mappings and settings are verified before pushing to production devices, as the **.utc** file includes structured ThinOS policies that are derived from the original JSON configuration, allowing for a seamless conversion process from JSON to ThinOS UTC using WMS.

Policy and package setup for ThinOS 10.x conversion

Explains how to configure policies and packages in WMS before and after converting DHC clients to ThinOS 10.x, ensuring all settings and packages apply correctly.

- Policy configuration before conversion:
 1. Configure policy and packages in WMS (same group) in DHC client.
 2. After DHC to ThinOS 10.x device conversion, all packages that are installed, and all configuration changes apply in the DHC Client.
- Policy Configuration after conversion:
 1. After DHC to ThinOS 10.x conversion, configure policy and packages in WMS (same group) in ThinOS 10.x device.
 2. All packages installed, and all configuration changes apply in the ThinOS 10.x device.

Migrating ThinOS 9.x policies to ThinOS 10.x using WMS

Learn how WMS admins migrate ThinOS 9.x group configurations to ThinOS 10.x using the Policy Migration Wizard, ensuring smooth transfer and consistent policies.


- Enhancement in UI for WMS **Groups & Configs** provides **Migrate ThinOS 9.x policies to ThinOS 10.x policies** migration link for a group. This feature is useful when ThinOS 9.x configurations are present and ThinOS 10.x configurations are not configured.
- WMS admin can use **Migrate ThinOS 9.x policies to ThinOS 10.x policies** feature to migrate all the group configuration from ThinOS 9.x to ThinOS 10.x. This feature also works for **Select groups** and to migrate child groups.
- The ThinOS 9.x to ThinOS 10.x configuration migration wizard displays warnings for ThinOS 9.x applications packages if the equivalent ThinOS 10.x packages are not present in WMS.
 - For **WMS cloud** customers, ThinOS 10.x packages are uploaded to the **Operator cloud**.
 - For **WMS on-premises Server** customers, ensure uploading ThinOS 10.x packages manually to the on-premises repository to avoid getting the migration wizard warnings.
- For configuring ThinOS 10.x configurations on a group from **Groups & Configs** UI using **Edit Policy**. When the ThinOS 9.x configurations are already present in the group, WMS displays a message. You can choose to use **Policy Migration Wizard** or proceed with configuring ThinOS 10.x configurations.
- WMS admin can check the option **Do not ask me again and open the ThinOS 10 Configuration page**. to disable the configuration wizard.
- WMS admin can enable the configuration wizard by following these steps: .
 - Go to **User Preferences > Policies**.
 - Select the checkbox: **Ask me if I want to use the ThinOS 10.x Policy Migration Wizard**.

NOTE: The ThinOS 9.x to ThinOS 10.x configuration migration wizard does not migrate firmware packages, BIOS, browser packages, and browser settings.

Migrating ThinOS 9.x configurations to ThinOS 10.x

Learn how WMS maps ThinOS 9.x configurations to ThinOS 10.x devices during upgrade or registration, excluding firmware and browser settings.

- When ThinOS 10.x devices register to WMS or upgrade from ThinOS 9.x to ThinOS 10.x without pre-configuration but have ThinOS 9.x configurations, the WMS server delivers the ThinOS 9.x configuration to the ThinOS 10.x devices.
- ThinOS 10.x devices using ThinOS 9.x configurations can be tracked on the **Device Details** page, where the **Device Policy Type** section appears as ThinOS 9.x.
- WMS admin can generate report for **Device Policy Type** for ThinOS 10.x devices from **Portal Admin > Reports** tab. If the ThinOS 9.x device has device level configurations, then upon upgrading to ThinOS 10.x, all existing ThinOS 9.x device level configurations are mapped to the ThinOS 10.x device automatically.

 **NOTE:** ThinOS 9.x firmware and ThinOS 9.x browser settings are not mapped to the ThinOS 10.x devices.

ThinOS 10.x system configuration and group management using WMS

Explains how to optimize device configuration groups in WMS for ThinOS 10.x, manage group changes, and handle firmware or package deployment prompts for efficient centralized management.

Key recommendations and behaviors:

- Use a minimal number of WMS groups and settings to support a wide range of unique device configurations.
- It applies to both multitenant and on-premises environments.
- When a thin client is moved to a different group in WMS, a message appears on the ThinOS 10.x device prompting the user to restart immediately or defer the restart until the next reboot to apply the new settings.
- Similarly, when deploying a new firmware or package using WMS, the thin client prompts the user to either begin installation immediately or delay it until the next reboot.

ThinOS 10.x configuration grouping using WMS

Describes how to organize and manage ThinOS 10.x configurations using group-based settings in WMS. Covers global, group, and device-level configurations, inheritance for child groups, and best practices for reducing redundancy and improving performance.

Key recommendations and behaviors:

- During deployment, evaluate the user must identify all required client configurations.
- During deployment, evaluate the user must identify all required client configurations.
- Other configurations—such as broker settings—may only apply to individual users on a device.
- Redundant or repeated configurations across devices can lead to performance issues and make updates harder to manage.
- Grouping configurations solves this problem by allowing shared settings across devices.
- In ThinOS 10.x, configuration inheritance means that child groups automatically inherit settings from their parent group.
- When creating groups, consider common device configuration criteria to simplify and streamline management.

Table 8. ThinOS 10.x configuration grouping overview

Group Types	Configurations
Global device configurations	<ul style="list-style-type: none">• Privilege Settings including Admin Mode• Security Policy Settings• Remote Control Settings (VNC)• Management Settings• All other global configurations
Device configurations for a group of clients	<ul style="list-style-type: none">• Group-based Broker Configurations• Group-based Printer Settings• Group-based Time Zone Settings

Table 8. ThinOS 10.x configuration grouping overview (continued)

Group Types	Configurations
Device configurations for a single device	<ul style="list-style-type: none"> • Client-based Terminal Name • Client-based Location • Client-based Location and Custom 1, 2, 3
Device configurations dynamically selected	ThinOS 10.x Select Group with device configurations

System variables

ThinOS uses system variables or part of a system variable when defining command values. System variables are often used to define unique values for fields such as terminal name or default user. For example, if the client has an IP address 123.123.123.022, `ACC&Right($FIP,3)` results in a value of ACC022. Using system variables makes it easier to manage groups of devices that require a unique terminal name or default user.

The following are the ThinOS 10.x system variables:

Table 9. ThinOS 10.x system variables

Variable	Description
\$IP	IP address
\$IPOCT4	The fourth octet of the IP Address, for example: if the IP address is 10.151.120.15, then the value is 15 .
\$MAC	Mac address
\$CMAC	Mac address with colon.
\$UMAC	Mac address with uppercase letters is used.
\$DHCP (extra_dhcp_option)	Extra DHCP options for ThinOS units, including 169, 140, 141, 166, and 167, are available to support advanced network configuration. For example, set a string test169 for the tag169 option in the DHCP server, and set TerminalName=\$DHCP(169) in the Wyse Management Suite policy. Check the terminal name in the UI, and the terminal name is test169 . 166 and 167 is default for the Wyse Management Suite MQTT Server and Wyse Management Suite CA validation in ThinOS. You must remap the options from the UI or the Wyse Management Suite policy if you want to use \$DHCP(166) or \$DHCP(167) .
\$DN	Sign on domain name
\$TN	Terminal name
\$UN	Sign on username
\$SUBNET	For subnet notation, the format is {network_address}_{network_mask_bits} . For example, if the IP address is 10.151.120.15, the network mask is 255.255.255.0, and 10.151.120.0_24 is used.
\$FIP	IP address is used in fixed format with three digits between separators. For example, 010.020.030.040.ini. Using it with the left or right modifier helps to define policy for the subnet. For example, <code>include=&Left(\$FIP,11).ini</code> is specified to include file 010.020.030.ini for subnet 010.020.030.xxx.
\$SN	Serial number or Service tag
\$VN	Version number
Right(\$xx, i) or and Left(\$xx, i)	Specifies that the variable is to be read from left or right. The \$xx is any of above parameters, and the parameter i specifies the digits for the offset of right or left.
&Right(\$xx, i) or &Left(\$xx, i)	Specifies whether the variable is read from left or right. The \$xx is any of the above System Variables. The option i specifies left or right offset digits. For example, in the parameter TerminalName=CLT-\$SN\$RIGHT\$07 , if the Serial Number (or Service Tag number) of the thin client is MA00256, the terminal name of the thin client is assigned as below:

Table 9. ThinOS 10.x system variables (continued)

Variable	Description
	<ul style="list-style-type: none">• First four characters—CLT-• The rest—The last right-most seven digits of the thin client serial number. The resulting terminal name is displayed as CLT-MA00256.
\$AT	Asset Tag must be enabled in the BIOS settings. \$AT can be used as terminal name, and the length is limited to 32 characters.

Managing BIOS settings for ThinOS devices

This chapter explains how to upgrade and configure BIOS settings for ThinOS 10.x devices using WMS or Admin Policy Tool, including password sync and platform-specific options.

Topics:

- [Upgrade BIOS using WMS](#)
- [BIOS setting configuration](#)
- [BIOS configuration details](#)

Upgrade BIOS using WMS

Explains how to upgrade the BIOS on ThinOS devices, use WMS or the Admin Policy Tool after the ThinOS image has been successfully updated.

Prerequisites

- Go to [Support | Dell](#), and download the latest BIOS file.
- If you are upgrading the BIOS using WMS, register the device to WMS.

For a successful upgrade, first upgrade the operating system image, then upgrade the BIOS. Upgrading both simultaneously causes the system to ignore the BIOS upgrade. The system then blocks installation of the same BIOS version, requiring an upgrade to a different version instead.

Steps

1. Open the Admin Policy Tool on the device or go to the ThinOS 10.x policy settings on WMS.
2. On the **Configuration Control | ThinOS** window, click the **Advanced** tab.
3. Expand **Firmware** and click **BIOS Firmware Updates**.
4. Click **Browse** and select the BIOS file to upload.
5. From the **Select the ThinOS BIOS to deploy** dropdown menu, select the BIOS file that you have uploaded.
6. Click **Save & Publish**.

The device restarts. BIOS is upgraded on your device.

i **NOTE:** For more information about the latest BIOS version, see the latest Dell Wyse ThinOS Operating System Release Notes at [Support | Dell](#).

i **NOTE:** BIOS upgrade requires a display screen (integrated or external) without which the update fails. In this case, you cannot install the BIOS package again. You must install another BIOS version.

If a power adapter is not connected on any ThinOS Mobile Client, the BIOS update fails. After the power adapter is connected, you must reboot to trigger the BIOS update again.

BIOS setting configuration

Explains how to configure BIOS on ThinOS devices by registering the device, setting a BIOS password, and using WMS or Admin Policy Tool to apply and publish changes for secure, standardized management.

Prerequisites

- If you are using WMS, ensure that you have registered the device and synchronize the BIOS admin password. The WDA stores the current BIOS password to unlock the BIOS and apply the required changes. For more information about using the **Sync BIOS Admin Password** option, see the *Dell Wyse Management Suite Administrator's Guide* at [Support | Dell](#).

- If you have not synced the BIOS password in the WMS server, you can input the current BIOS password in BIOS policy to publish BIOS settings. If you have synced the BIOS password in the WMS server, the **Current BIOS Admin password** option in the BIOS policy is ignored. WMS server uses the synced BIOS password to publish BIOS settings.
- If you are using the Admin Policy Tool, ensure that you enter the current BIOS admin password in the **Advanced > BIOS** section.

Steps

1. Open the Admin Policy Tool on the device or go to the ThinOS 10.x policy settings on WMS.
2. In the **Configuration Control | ThinOS** window, click the **Advanced** tab.
3. Expand **BIOS** and select your preferred platform.
4. In the **System Configuration** section, modify the USB ports and audio settings.
5. In the **Security** section, modify the administrator-related configurations.
6. In the **Power Management** section, modify the power-saving options.
7. In the **POST Behavior** section, modify the post behavior options.
8. Click **Save & Publish**.

NOTE: If the BIOS does not have a password and you set a new one, or if you change the BIOS password using a select group, a reboot is required for the new password to take effect, while other BIOS setting changes are applied after a second reboot.

NOTE: If you enable **Set Admin Password**, set a new BIOS password, and then reboot the thin client, the new password is automatically synced to the WMS server. However, if you enable **Set Admin Password**, set the password, and then disable the option before rebooting, the BIOS password is cleared and reset to empty.

NOTE: On ThinOS clients, the **Current BIOS Admin Password** option is always blank, and the **Set Admin Password** option is always disabled. These options do not have any impact on the functionality.

BIOS configuration details

The BIOS Common Configuration acts as a centralized settings page in ThinOS that consolidates all BIOS settings that are supported across all ThinOS 10.x devices. This feature ensures consistent BIOS configurations across devices using the same Active Directory in WMS.

To access the BIOS Common Configuration settings in WMS, go to **Advanced Settings > BIOS Common Configurations > Dell Supported Devices BIOS Settings**.

The following are the key highlights:

- If a platform-specific BIOS configuration exists, that configuration is applied; otherwise, the common BIOS configuration is used.
- Platform-specific settings take precedence over common settings.
- Supports scalable BIOS configuration across many devices.
- Reduces manual effort during deployment by allowing BIOS settings to be pushed centrally.
- Enables easier onboarding of new platforms by falling back to a common configuration until platform-specific values are available.

NOTE: This feature is supported across all platforms. However, if a platform includes a dedicated BIOS settings page, any changes made there overrides the BIOS Common Configuration settings.

Table 10. Supported Configuration

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
Boot Options				
Enable USB Boot Support	Enable/Disable	Enables booting to USB mass storage devices. Disabling prevents this. Does not affect OS-level USB access.	All Devices	Not applicable

Table 10. Supported Configuration (continued)

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
PXE Boot Support	Enable/Disable	Allows the device to perform a PXE Boot.	All Devices	Not applicable
USB Port Control				
Enable Rear USB Ports	Enable/Disable	Enables rear USB ports.	3040, OptiPlex 3000 and Wyse 5070 only	Not applicable
Enable USB port Front Top	Enable/Disable	Enables the front top USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	OptiPlex Micro-Plus 7010, Wyse 5070, OptiPlex 3000	Not applicable
Enable USB port Front Medium	Enable/Disable	Enables front medium USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	Wyse 5070	Not applicable
Enable USB port Front Bottom	Enable/Disable	Enables the front bottom USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	OptiPlex Micro-Plus 7010, Wyse 5070, OptiPlex 3000	Not applicable
Enable Side USB Ports	Enable/Disable	Enables USB ports on the side of AIO. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Not applicable
Enable Side USB port Top	Enable/Disable	Enables top-side USB port on AIO. Keyboard and mouse work in BIOS setup irrespective of this setting.	5400 AIO and 5470 AIO	Enable Side USB Ports
Enable Side USB port Bottom	Enable/Disable	Enables bottom-side USB port on AIO. Keyboard and mouse work in BIOS setup irrespective of this setting.	5400 AIO and 5470 AIO	Enable Side USB Ports
Enable Rear USB port Top Left	Enable/Disable	Enables rear upper left USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Enable Rear USB port Top Right	Enable/Disable	Enables rear upper right USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Enable Rear USB port Bottom Left	Enable/Disable	Enables rear bottom left USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports

Table 10. Supported Configuration (continued)

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
Enable Rear USB port Bottom Right	Enable/Disable	Enables rear bottom right USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Audio				
Audio	Enable/Disable	Enables integrated audio controller.	All Devices	Not applicable
Security				
Current BIOS Admin Password	Password Value	Required to edit BIOS settings. If previously synced, the displayed value may differ.	All Devices	Required to make any change
Set New BIOS Admin Password	Enable/Disable	Enables BIOS administrator password. The changes take effect immediately.	All Devices	Not applicable
New BIOS Admin Password	Password Value	Set the new admin password. Must contain at least one digit, one uppercase, one lowercase, and one special character.	All Devices	Set New BIOS Admin Password
Admin Setup Lockout	Enable/Disable	Prevents access to BIOS Setup when the admin password is set.	All Devices	Not applicable
Power Management				
Auto On Time	Disable, Daily, Workday, Days	BIOS uses UTC (0) time zone. Set UTC-based time, not operating system time.	All Devices	Not applicable
Time	Time Value	BIOS uses UTC (0) time. Set UTC-based time, not operating system time.	All Devices	Auto On Time
Days	Day List	Set specific days to auto power on.	All Devices	Auto On Time
Wake-on-LAN	LAN only, LAN with PXE Boot, Disable	Allows wake from shutdown using LAN or wireless LAN signal.	All Devices	Not applicable
AC Recovery	Power Off, Power On, Last State	Behavior after AC power is restored.	All Devices	Not applicable
Wake On USB	Enable/Disable	Enables USB to wake the system from its hibernate state.	All Devices	Not applicable
Deep Sleep Control	Enabled in S5 only/S4 and S5	Controls system power conservation in shutdown (S5) or hibernate (S4).	All Devices	Not applicable

Table 10. Supported Configuration (continued)

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
POST Behavior				
MAC Address Pass Through	Passthrough MAC, Disabled, NIC 1 MAC	Replaces NIC MAC with selected MAC address.	All Devices	Not applicable
BIOS POST Behavior				
Fastboot	Minimal, Auto, Thorough	Speeds up boot by skipping compatibility steps.	All Devices	Not applicable
Extend BIOS Post Time	0 / 5 / 10 seconds	Adds a delay before boot to allow reading POST messages.	All Devices	Not applicable
Keyboard Error Detection	Enable/Disable	Specifies if keyboard errors are reported during boot.	All Devices	Not applicable
BIOS Pre behavior				
Suppress Docking Station Warning Msg	Enable/Disable	Suppresses boot warning message for incompatible device that is connected to DockPort.	All Devices	Not applicable
Virtualization Support				
Enable Virtualization	Enable/Disable	Enables Virtualization Technology (VT).	All Devices	Not applicable
Enable Virtualization for Direct I/O	Enable/Disable	Enables VT for Direct I/O.	All Devices	Not applicable

Removing unused packages and optimizing ThinOS system performance

This chapter explains how to clean up and optimize ThinOS 10.x systems by removing unused application packages using WMS or Admin Policy Tool to maintain system performance and clarity.

Topics:


- [Delete ThinOS 10.x application packages using Admin Policy Tool](#)
- [Delete ThinOS 10.x application packages using WMS](#)

Delete ThinOS 10.x application packages using Admin Policy Tool

Explains how to remove ThinOS 10.x packages using the device UI or Admin Policy Tool, for single or multiple packages.

Steps

1. Log in to the ThinOS 10.x device.
2. From the system menu, go to **System Tools > Packages**. All the installed ThinOS 10.x packages are listed.
3. Select a package that you want to delete and click **Delete**.

 **NOTE:** To delete all the packages, click **Delete all**.

4. Click **OK** to save your settings.

Delete ThinOS 10.x application packages using WMS


Explains how to uninstall ThinOS 10.x application packages using WMS by selecting packages in group policies, using the Standard or Advanced tabs, and publishing the changes for managed devices.

Prerequisites


- Create a group in WMS with a group token.
- Register the device to WMS.

Steps


1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 10.x**. The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.

 **NOTE:** If you cannot locate the Application Package option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse** and select the application package to upload.
6. For each category, ensure that the switch is set to **UNINSTALL**. You can select only one version in the list for each category.

 **NOTE:** For a given ThinOS release, you can install only the supported packages that are mentioned in the corresponding ThinOS Release Notes available at [Support | Dell](#).

7. Click **Save & Publish**.

 **NOTE:** For the **Other** category, you can select multiple application packages and versions, as the packages are not predefined. However, the **UNINSTALL** option is not supported for this category. After adding application packages to the **Other** category, it is recommended to upgrade the WMS configUI. The updated configUI automatically assigns the application packages to the appropriate new category.

Support Resources

This chapter provides FAQs, and support resources for resolving ThinOS 10.x migration issues, including DHCP/DNS setup and log collection.

Topics:

- [FAQs](#)
- [Log collection](#)
- [Resources and support](#)
- [Reference materials and supporting documentation](#)
- [Contacting Dell](#)

FAQs

How do I verify if my device can be converted to ThinOS 10.x?

You can refer to the ThinOS 10.x Hardware Compatibility List (HCL) document at [Support | Dell](#) to check if your device is supported. If your device is not listed, you can run the ThinOS 10.x Compatibility Checker to assess whether it meets the minimum hardware requirements for conversion.

For more information about other ThinOS 10.x document details, see [Reference materials and supporting documentation](#).

How to create and configure DHCP option tags?

Steps

1. Open the Server Manager.
2. Go to **Tools**, and click **DHCP option**.
3. Go to **FQDN > IPv4**, and right-click **IPv4**.
4. Click **Set Predefined Options**.
The **Predefined Options and Values** window is displayed.
5. From the **Option class** drop-down list, select the **DHCP Standard Option** value.
6. Click **Add**.
The **Option Type** window is displayed.
7. Configure the required DHCP option tags.
 - To create the 165 Wyse Management Suite server URL option tag, do the following:
 - a. Enter the following values, and click **OK**.
 - Name—WMS
 - Data type—String
 - Code—165
 - Description—WMS_Server
 - b. Enter the following value, and then click **OK**.
String—WMS FQDN
 - To create the 166 MQTT server URL option tag, do the following:
 - a. Enter the following values, and click **OK**.
 - Name—MQTT
 - Data type—String
 - Code—166
 - Description—MQTT Server

b. Enter the following value, and click **OK**.

String—MQTT FQDN. For example, **WMSServerName.YourDomain.Com:1883**

- To create the 167 Wyse Management Suite CA Validation server URL option tag, do the following:

a. Enter the following values, and click **OK**.

- Name—CA Validation
- Data type—String
- Code—167
- Description—CA Validation

b. Enter the following values, and click **OK**.

String—TRUE or FALSE

- To create the 199 Wyse Management Suite Group Token server URL option tag, do the following:

a. Enter the following values, and click **OK**.

- Name—Group Token
- Data type—String
- Code—199
- Description—Group Token

b. Enter the following values, and click **OK**.

String—defa-quarantine



NOTE: The options must be either added to the server options of the DHCP server or scope options of the DHCP scope.

How to create and configure DNS SRV records?

Steps

1. Open the Server Manager.
2. Go to **Tools**, and click **DNS**.
3. Go to **DNS > DNS Server Host Name > Forward Lookup Zones > Domain > _tcp**, and right-click the **_tcp** option.
4. Click **Other New Records**.
The **Resource Record Type** window is displayed.
5. Select the **Service Location (SRV)**, click **Create Record**, and do the following:
 - a. To create Wyse Management Suite server record, enter the following details and click **OK**.
 - Service—_WMS_MGMT
 - Protocol—_tcp
 - Port number—443
 - Host offering this service—FQDN of WMS server
 - b. To create MQTT server record, enter the following values, and then click **OK**.
 - Service—_WMS_MQTT
 - Protocol—_tcp
 - Port number—1883
 - Host offering this service—FQDN of MQTT server
6. Go to **DNS > DNS Server Host Name > Forward Lookup Zones > Domain**, and right-click the domain.
7. Click **Other New Records**.
8. Select **Text (TXT)**, click **Create Record**, and do the following:
 - a. To create Wyse Management Suite Group Token record, enter the following values, and click **OK**.
 - Record name—_WMS_GROUPTOKEN
 - Text—WMS Group token
 - b. To create Wyse Management Suite CA validation record, enter the following values, and then click **OK**.
 - Record name—_WMS_CAVALIDATION
 - Text—TRUE/FALSE

How to retrieve secure WMS and Group Registration Key?

To retrieve the secure WMS server and secure Group Registration Key, do the following:

Steps

1. Go to **WMS server > Portal Administration > Console Settings > WMS Discovery**.
2. Enter the group token.
3. Select **DNS** from the **Discovery Type** drop-down menu.
4. Click **Generate Details**.

Log collection

To facilitate efficient troubleshooting and issue resolution, system logs must be collected and packaged. This process involves gathering relevant operating system logs, event traces, configuration files, and error reports that capture the system's behavior during the issue. These logs provide critical insights for root cause analysis.

Error logs for ThinOS 10.x devices

This table provides a solution guide to resolve common error logs and troubleshoot issues that are related to ThinOS 10.x devices.

Table 11. Error Log table

Error Log	Resolution
No AC plugged in	Plug in power adapter, reschedule job
Platform Not Supported	This hardware platform is not supported
Error mounting recovery partition	The Ubuntu image is not a factory image. Reinstall the factory image.
No DHC/ThinOS package in recovery partition	Cannot find the ThinOS image, reschedule job
Error in extracting DHC/ThinOS 10.x future packages	Failed to extract the ThinOS image, reschedule job
Error copying the DHC/ThinOS 10.x future packages to recovery partition	Failed to copy the ThinOS image, reschedule job
ThinOS 10.x package verification failed	ThinOS image is not correct, reschedule job with the correct ThinOS image
Not enough space in Recovery Partition	Clear the recovery partition
The free space of Recovery Partition is not enough	Clear the recovery partition

Resources and support

Accessing documents using the product search

1. Go to [Support | Dell](#).
2. In the **Identify a product or ask support** search box, enter a product identifier, for example, **Dell Pro 14 PC14250** or **Dell Pro 24 All-in-One QC24251** and click **Search**.
A list of matching products is displayed.
3. Select your product.
4. Click **Support Resources > Manuals & Documents**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to [Support | Dell](#).
2. Click **Browse All Products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **Wyse Software**.
6. Click **Dell ThinOS**.
7. Click **Select This Product**.
8. Click **Support Resources > Manuals & Documents**.

Reference materials and supporting documentation

This chapter serves as a centralized repository of official Dell ThinOS 10.x documentation. It enables administrators to quickly access key resources for deployment, configuration, compatibility validation, and customization. It provides direct access to key Dell ThinOS 10.x documents that assist IT administrators in various aspects of endpoint management.

Table 12. Document index

Document title	Description	Go to
Dell ThinOS 10.x 2502, 2505, and 2508 Administrator Guide	Provides IT administrators with instructions for configuring, managing, and troubleshooting the system.	Dell ThinOS documentation page
Dell ThinOS 10.x 2502, 2505, and 2508 Migration Guide	Provides IT administrators with procedures for migrating data, applications, or systems from one environment to another.	
Dell ThinOS 10.x 2502, 2505, and 2508 Release Notes	Provides users with a summary of new features, bug fixes, and known issues for a software release.	
Dell ThinOS 10.x Hardware Compatibility List	Provides IT administrators with details on compatible hardware, software, and supported configurations for the software.	
Dell ThinOS 10.x Compatibility Checker User Guide	Provides IT administrators with the details to repurpose any Dell or non-Dell hardware for ThinOS 10.x using a USB imaging method.	
Dell ThinOS 10.x App Builder User's Guide	Provides users with instructions for using the software, including setup and features.	

Contacting Dell

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

Dell provides several online and telephone-based support and service options. Availability varies by country or region and product, and some services may not be available in your area. To contact Dell sales, technical support, or customer service issues, follow the steps.

1. Go to [Support | Dell](#).
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.

4. Select the appropriate service or support link based on your need.

Appendix: Reference and licensing

This chapter lists abbreviations, licensing instructions, and ThinOS 10.x application packages to support administrators in managing deployments and compliance.

Topics:

- [Abbreviations](#)
- [ThinOS 10.x 2508 application packages](#)
- [Returning unused ThinOS subscription licenses](#)
- [ThinOS 10.x subscriptions allocation](#)

Abbreviations

This chapter lists ThinOS 10.x application packages and includes abbreviations and system terms that are used throughout the document. It supports IT administrators in identifying and managing relevant components across platforms.

Table 13. Abbreviations

Short Form	Full Form
WMS	Wyse Management Suite
DHC	Dell Hybrid Client
DCA	Dell Client Agent
WDA	Wyse Device Agent
TAL	ThinOS Activation License
MQTT	Message Queuing Telemetry Transport
UI	User Interface
UX	User Experience
BIOS	Basic Input/Output System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
SRV	Service Record
OOBE	Out-of-Box Experience
ISO	Disk Image File (contextually referring to OS install package format)
CA	Certificate Authority
TPM	Trusted Platform Module
SN	Serial Number
MAC	Media Access Control address
IP	Internet Protocol
AT	Asset Tag

ThinOS 10.x 2508 application packages

For ThinOS 10.x 2508, you can install the latest application packages that are mentioned in the following table:

Table 14. ThinOS 10.x 2508 packages

ThinOS packages	ThinOS application package details
Amazon_WorkSpaces_Client	Amazon_WorkSpaces_Client_2024.8.5230.106_T10.pkg
App_Builder	App_Builder_2.0.37_T10.pkg
CI_Software_Enabler	CI_Apps_Enabler_28.3.2.23_T10.pkg
Cisco_Jabber	Cisco_Jabber_15.1.104_T10.pkg
Cisco_Webex_App_VDI	Cisco_Webex_App_VDI_45.6.1.32593.104_T10.pkg
Cisco_Webex_Meetings_VDI	Cisco_Webex_Meetings_VDI_45.2.1.2.102_T10.pkg
Citrix_Workspace_App	Citrix_Workspace_App_25.03.0.66.11_T10.pkg
ControlUp_VDI_Agent	ControlUp_VDI_Agent_2.4.2506.4.36_T10.pkg
DellDock_WD19_WD22_PFW	DellDock_WD19_WD22_PFW_01.04.70_T10.pkg
Dell Monitor Firmware Upgrade	U2724DE_PFW_103.5_T10.pkg
DHC_Ubuntu_To_ThinOS10_conversion	DellHybridClient_Ubuntu_To_ThinOS10_conversion_2508_10.0127.tar
eG_VM_Agent	eG_VM_Agent_7.5.2.100_T10.pkg
Epos_Connect	Epos_Connect_8.0.0.48071.99_T10.pkg
Firefox	Firefox_128.13.0.128_T10.pkg
Google_Chrome	Google_Chrome_138.0.7204.183.146_T10.pkg
HID_Fingerprint_Reader	HID_Fingerprint_Reader_210217.23.101_T10.pkg
Identity_Automation_QwickAccess	Identity_Automation_QwickAccess_2.1.1.106_T10.pkg
Imprivata_PIE	Imprivata_PIE_23.3.0.715913.107_T10.pkg
Jabra	Jabra_8.5.10.111_T10.pkg
Lakeside_Virtual_Agent	Lakeside_Virtual_Agent_99.0.0.175.102_T10.pkg
Liquidware_Stratusphere_Ux_Connector_ID_Agent	Liquidware_Stratusphere_Ux_Connector_ID_Agent_6.7.0.79.96_T10.pkg
Microsoft_AVD	Microsoft_AVD_3.2.207_T10.pkg
RingCentral_App_VMware_Plugin	RingCentral_App_VMware_Plugin_25.2.30.104_T10.pkg
RootOS	Root_2508.10_0127_signed.pkg
	Root_2508.10_0127_signed.pkg
RootOS_Downgrade	RootOSDowngrade_2508.10.0127_T10.pkg
TelegrafAgent	TelegrafAgent_1.35.2.1.40_T10.pkg
ThinOS_Telemetry_Dashboard	ThinOS_Telemetry_Dashboard_1.1.0.100_T10.pkg
USB image	ThinOS10_2508_0127.iso
uxm_Endpoint_Agent	uxm_Endpoint_Agent_2025.07.03.100_T10.pkg
OmniSSA_Horizon_ClientSDK	OmniSSA_Horizon_ClientSDK_2506.8.16.0.250_T10.pkg
Zoom_Universal	Zoom_Universal_6.4.11.26350.107_T10.pkg

Returning unused ThinOS subscription licenses

You can return unused or unallocated ThinOS 10 subscription licenses from a private WMS Pro server back to the public cloud. This applies to:

- ThinOS 10 Subscription–Dell Client
- ThinOS 10 Subscriptions–Third Party Client
- Dell Hybrid Client seats
- Thin Client seats

You can return the licenses using any of the following two methods:

- [Online activation](#)
- [Offline key exchange](#)

Online activation of license key

Return unused licenses by reimporting a reduced license count from the public cloud into the WMS on-premises server using global admin credentials.

Steps

1. Log in to the WMS on-premises environment.
2. Go to **Portal Administration > Subscription**.
3. In the **Import License** section:
 - a. Enter your public cloud global administrator credentials.
 - b. Specify the updated number of **ThinOS 10 Subscriptions - Dell Client**.
4. Click **Import**.

Example

For example, if you initially import 10 ThinOS 10 Subscriptions – Dell Client and later reduce the number to 7 during a second import, the remaining three licenses are automatically returned to the public cloud.

Offline exchange of license key

Export a license key from the public cloud with a reduced license count and apply it manually to the WMS on-premises server using the on-premises Identifier.

Steps

1. Log in to the WMS public cloud environment as a global administrator.
2. Go to **Portal Administration > Subscription**.
3. In the **Export License For Private Cloud** section, enter the updated **Number of ThinOS 10 Subscriptions - Dell Client** and provide the **On-Prem Identifier** from which the license must be returned.
4. Click **Export** and copy the key.
5. Paste the key into the WMS on-premises server.





Example

For example, if you initially export 10 ThinOS 10 Subscriptions – Dell Client and later export only 7 using the same on-premises Identifier, the remaining three licenses are returned to the public cloud.

ThinOS 10.x subscriptions allocation

You can allocate the ThinOS devices subscriptions between Wyse Management Suite Private Cloud and Wyse Management Suite Public Cloud account.

Steps

1. Log in to the Wyse Management Suite Public Cloud console.
2. Go to **Portal Administration > Accounts > Subscription**.
3. Enter the number of thin client seats.
 **NOTE:** The thin client seats should be manageable in the Public Cloud. The entered number of thin client seats must not exceed the number that is displayed in the Manageable option.
4. Click **Export**.
 **NOTE:** The number of Public Cloud subscriptions is adjusted based on the number of thin client seats that are exported to the Private Cloud.
5. Copy the generated subscription key.
6. Log in to Wyse Management Suite Private Cloud console.
7. Go to **Portal Administration > Accounts > Subscription**.
8. Import the exported subscription key to the Private Cloud.
 **NOTE:** The subscription cannot be imported if it has insufficient thin client seats to manage the number of devices being managed in the Private Cloud. In this case repeat steps 3–8 to allocate the thin client seats.
9. Verify that the total number of ThinOS 10.x seats matches or exceeds the number of ThinOS devices being managed.
10. Ensure that each converted or newly deployed ThinOS 10.x device is successfully registered to WMS and obtains a valid subscription from the server.
11. During device conversion (from Windows, Dell Hybrid Client, or Ubuntu 24.04 for Managed Clients):
 - Confirm that ThinOS 10.x subscriptions are available in the WMS console.
 - Devices without available subscriptions may enter an unlicensed state and cannot be fully managed until additional seats are imported.
 **NOTE:** From Wyse Management Suite 3.2, older Wyse Management Suite server cannot be activated online from public cloud.