

# **Dell ThinOS 10.x 2502 and 2505**

## 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.

|   |           |
|---|-----------|
| <b>Chapter 1: Introduction.....</b>   | <b>5</b>  |
| Supported platforms.....  | 5         |
| Supported Wyse Management Suite versions.....   | 6         |
| Support scenarios for ThinOS 10.x.....  | 6         |
| Upload the package using Groups & Configs.....  | 8         |
| Upload the package using the Apps & Data .....  | 9         |
| Upload the package using local/remote repository.....                                     | 9         |
| <b>Chapter 2: Download ThinOS firmware, BIOS, and application packages.....</b>           | <b>10</b> |
| File naming convention.....   | 13        |
| <b>Chapter 3: Upgrading ThinOS firmware.....</b>  | <b>14</b> |
| Important notes.....  | 14        |
| Upgrade ThinOS 9.x to ThinOS 10.x using Wyse Management Suite.....                        | 14        |
| Upload and push ThinOS application packages.....  | 15        |
| Download ThinOS 10 ISO image.....   | 16        |
| Install ThinOS from USB drive using Dell OS Recovery Tool.....                            | 17        |
| Install ThinOS from USB drive for non-Dell platform.....                                  | 25        |
| <b>Chapter 4: Register Ubuntu + DCA as Generic Client to Wyse Management Suite.....</b>   | <b>26</b> |
| Register Ubuntu + DCA as Generic Client to Wyse Management Suite manually.....            | 26        |
| Register Ubuntu + DCA as Generic Client by using DHCP option tags or DNS SRV records..... | 27        |
| <b>Chapter 5: Wyse Management Suite Environment with DHCP and DNS Auto Discovery.....</b> | <b>28</b> |
| Register ThinOS 10.x devices with IPv4 DHCP option tags.....                              | 29        |
| WMS auto discovery by IPv6 DHCP option.....   | 30        |
| Configure devices with DNS SRV record.....  | 31        |
| <b>Chapter 6: Register ThinOS 10.x devices using Wyse Device Agent.....</b>               | <b>32</b> |
| <b>Chapter 7: Converting to ThinOS 10.....</b>  | <b>33</b> |
| Convert Dell Hybrid Client to ThinOS 10.....  | 33        |
| Policy configuration.....   | 34        |
| Error logs for ThinOS 10.x devices.....   | 34        |
| Convert systems with Dell Ubuntu for managed clients.....                                 | 35        |
| <b>Chapter 8: Configuring a ThinOS 10.x client using Wyse Management Suite .....</b>      | <b>37</b> |
| ThinOS 10 configuration grouping overview.....  | 37        |
| ThinOS 10 system variables.....   | 37        |
| <b>Chapter 9: BIOS Installation.....</b>  | <b>39</b> |
| Upgrade BIOS.....   | 39        |
| Edit BIOS settings.....   | 39        |

**Chapter 10: Delete ThinOS 10 application packages.....41**

**Chapter 11: Resources and support.....42**

**Chapter 12: Contacting Dell.....43**

# Introduction


This guide provides instructions to migrate from ThinOS 9.x version 2408 or later and Dell Hybrid Client/Dell Ubuntu to ThinOS 10.x 2502 or 2505 using Wyse Management Suite 5.2 or later.


The migration process includes the following tasks:


1. Register the Thin Client with Wyse Management Suite by automating the discovery of the Wyse Management Suite server and Group Registration Token using DHCP or DNS records.
2. Download the ThinOS 10.x firmware from the [Support | Dell](#) site—see [Download the ThinOS firmware, BIOS, and application packages](#).
3. Install ThinOS 10.x from a USB drive using Dell OS Recovery Tool—see [Install ThinOS from USB drive using Dell OS Recovery Tool](#).
4. Convert Dell Ubuntu to ThinOS 10 using Wyse Management Suite version 5.0 or later—see [Convert systems with Dell Ubuntu for managed clients](#).
5. Configure the ThinOS 10.x based device using Wyse Management Suite version 5.0 or later—see [Upgrading ThinOS 10.x client using Wyse Management Suite](#).
6. Migrate Dell Hybrid Client devices to ThinOS 10.x using Wyse Management Suite version 5.0 or later—see [Convert Dell Hybrid Client to ThinOS 10](#).
7. Migrate the ThinOS 9.x-based device to ThinOS 10.x—see [Support scenarios for ThinOS 10.x](#).

When converting a device from a different operating system to ThinOS 10.x 2502 or ThinOS 10.x 2505, or when installing the ThinOS 10.x 2502 (10.0052) or ThinOS 10.x 2505 recovery image, ThinOS 10.x sets the following BIOS settings during the initial boot:

**Table 1. BIOS settings during the initial boot**

| BIOS setting               | Value   |
|----------------------------|---|
| BIOS password              | <b>Fireport</b>   |
| SATA/NVMe Operation        | <b>AHCI/NVMe</b>  |
| Integrated network adapter | Set to <b>Enabled</b> (set to disable PXE boot support)   |
| Wake-on-LAN                | <b>LAN only</b><br> <b>NOTE:</b> For OptiPlex 3000 Thin Client with SFP module, the option is set to <b>LAN or SFP NIC</b> . |
| Enable Secure Boot         | <b>ON</b>   |
| Enable USB Boot Support    | <b>OFF</b>  |
| Enable USB Wake Support    | <b>ON</b>   |
| Deep Sleep Control         | <b>Disabled</b>   |

 **NOTE:** These BIOS settings are applicable only to devices where the BIOS password is set to **Fireport** or if the password is not set.


 **NOTE:** BIOS settings are not automatically applied during initial boot on non-Dell platforms.

## Supported platforms

The Dell ThinOS 10.x firmware is supported on the following Dell and non-Dell platforms:

**Table 2. Dell and non-Dell platforms**

| Supported platforms | Model   |
|---------------------|---|
| Thin Clients        | <ul style="list-style-type: none"><li>• Wyse 5070 Thin Client</li><li>• Wyse 5070 Extended Thin Client</li><li>• Wyse 5470</li><li>• Wyse 5470 All-in-One</li></ul>   |
| OptiPlex            | <ul style="list-style-type: none"><li>• OptiPlex 3000 Thin Client</li><li>• OptiPlex 5400 All-in-One</li><li>• OptiPlex All-In-One 7410</li><li>• OptiPlex All-in-One 7420</li><li>• OptiPlex Micro Plus 7010</li></ul> |
| Latitude devices    | <ul style="list-style-type: none"><li>• Latitude 3420</li><li>• Latitude 3440</li><li>• Latitude 5440</li><li>• Latitude 5450</li><li>• Latitude 5540</li><li>• Latitude 5550</li></ul>                                 |
| Dell Pro series     | <ul style="list-style-type: none"><li>• Dell Pro Rugged 13 RA13250</li><li>• Dell Pro Rugged 14 RB14250</li><li>• Dell Pro 16 Plus PB16250</li><li>• Dell Pro 14 PC14250</li><li>• Dell Pro 24 All-in-One</li></ul>     |
| Non-Dell platform   | Amulet Hotkey (DX 5 series)   |


 **NOTE:** The minimum supported configuration for ThinOS 10.x is 32 GB storage and 8 GB RAM. ThinOS 10.x supported platforms do not support Intel i7 processors.

 **NOTE:** Firmware upgrade from ThinOS 9 to ThinOS 10 is not supported on devices with 4 GB RAM.

## Supported Wyse Management Suite versions

ThinOS 10.x is supported on Wyse Management Suite version 5.0 or later.

Wyse Management Suite default communications are handled over port 443. The Wyse Management Suite server address must be specified either directly in the ThinOS user interface or provided through DHCP or DNS configuration.

 **NOTE:** To download the Wyse Management Suite Standard edition or start a Pro trial, go to [Wyse Management Suite](#) page. For product documentation, go to the Wyse Management Suite product page at [Support | Dell](#).

## Support scenarios for ThinOS 10.x

### Support for ThinOS 10.x device management

- WMS is enabled to support ThinOS 10.x device registration, heartbeat, check-in, and other real time commands that are supported in ThinOS 9.x.
- A new section in **Group & Configs > Edit Policy** is added for ThinOS 10.x device configuration. ThinOS 10.x devices can be configured from device group level, select group level, user group level, device level, and user level.
- WMS features for ThinOS 9.x such as Wave configuration, Device Exception To Override Select Group Policy, and all ThinOS 9.x supported real time commands, and IPv6 support are extended to support the ThinOS 10.x devices.

## Support for ThinOS 10.x package management

- For cloud environment, ThinOS 10.x Applications, BIOS, and Firmware packages are available in the public cloud, such as **Operator cloud** and **Tenant cloud**.
- 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](#)
- NOTE:** The ThinOS 9.x to ThinOS 10.x upgrade package upload fails on a **WMS on-premises Server** with 8 GB RAM. Ensure that the WMS server has 16 GB RAM to upload ThinOS 9.x to ThinOS 10.x upgrade package.

## Support for ThinOS 10.x device licensing

- ThinOS 9.x devices that are upgraded to ThinOS 10.x using a factory image or BIOS-injected key do not require an **OS Activation** key from the WMS server for ThinOS 10.x client functionality.
- ThinOS 9.x devices upgraded to ThinOS 10.x use the existing ThinOS 9.x Activation License.
- Dell Hybrid Client devices converted to ThinOS 10.x continue to use the existing Dell Hybrid Client license. When the Dell Hybrid Client license expires, the device requires a ThinOS 10.x Activation license for activation.
- Any device which is converted to ThinOS 10.x using an ISO image or USB device continues to use the Dell Hybrid Client license if the active license is present in WMS. If the Dell Hybrid Client license is not present, then the ThinOS 10.x Activation license is used. If both Dell Hybrid Client license and ThinOS 10.x OS Activation license are not present in WMS, then the ThinOS 10.x device functionality enters a locked state.
- NOTE:** If no DHC or ThinOS 10.x activation license is available, the device continues to work for 30 days. After that, it is no longer be possible to push any configurations from the WMS.

See the table for a concise overview of the different license scenarios and their effects:


**Table 3. ThinOS license scenarios**

| License Type  | Scenario  | Post Conversion                                     | On DeviceUnregister          | Can the License Expire?                 | On License Expiry                           |
|---|---|---|------------------------------|---|---|
| BIOS injected Security Key  | ThinOS 9.x & 10.x factory installed devices   | The device does not need any additional license     | N/A                          | Never                                   | N/A   |
| ThinOS Activation License (TAL)   | ThinOS 9.x to ThinOS 10.x conversion  | The device requests a license from WMS and cache it | Never deletes cached license | Never                                   | N/A   |
| DHC Device License  | DHC to ThinOS 10.x  | The device requests a license from WMS and cache it | Never deletes cached license | Yes, it is a subscription-based license | The Device requests WMS for license renewal |
| ThinOS 10 Subscription – Third Party Client licenses (for non-Dell devices) | <ul style="list-style-type: none"><li>Dell Ubuntu to ThinOS 10</li><li>Offline Imaging (USB Imaging) using Dell Recovery Tool</li></ul> | The device requests a license from WMS and cache it | Never deletes cached license | Yes, it is a subscription-based license | The Device requests WMS for license renewal |

- NOTE:** Once the license expires, a watermark message appears on top of all VDI session windows, and a warning message is displayed on the login window until the license is renewed.


## Support for ThinOS 9.x configuration migration to ThinOS 10.x

- 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.

## Support for ThinOS 9.x WMS UI or UX migration to ThinOS 10.x

- 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.


## Upload the package using Groups & Configs

### About this task

ThinOS 10.x firmware, application, and BIOS packages can be uploaded and deployed using the **Groups & Configs**.

### 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 the Apps & Data

### About this task

ThinOS 10.x firmware, application, BIOS packages can be uploaded and deployed using the **Apps & Data**.

To upload and deploy the package, do the following:

### 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

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.

## Download ThinOS firmware, BIOS, and application packages

This section 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 the [Support | Dell](#) site.
2. In the **Identify a product or ask support** search box, enter a product identifier, for example, **OptiPlex 3000 Thin Client** or **OptiPlex All-In-One 7410** and click **Search**.  
A list of matching products is displayed.
3. Select your product.
4. On the product support page, click **Drivers & Downloads**.
5. Select the **Operating System** as **ThinOS 10**.
6. Locate the required ThinOS Image entry and click **Download**.

**Table 4. Available ThinOS 10.x 2505 package options**

| Scenario   | ThinOS 10 package title  |
|--|--|
| Upgrade from ThinOS 10 to ThinOS 10 (same version family)      | ThinOS 10 2505.76 Firmware Upgrade Package                                     |
| Convert Dell Hybrid Client or Dell Ubuntu Base OS to ThinOS 10 | Dell Hybrid Client/Ubuntu Managed Clients to ThinOS 10 2505 Conversion Package |
| Download Dell Recovery Image                                   | ThinOS 10 2502 Offline USB Installer Package                                   |
| Upgrade from ThinOS 9.5.3102 or later to ThinOS 10.0052        | ThinOS 9.5.3102 or later to ThinOS 10 2505 Upgrade Package                     |

7. To use ThinOS packages, select the package and click **Download**.

**Table 5. ThinOS 10 packages**

| ThinOS 10 packages        | ThinOS image title  |
|---------------------------|---|
| Citrix_Workspace_App      | Citrix package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).         |
| VMware_Horizon_Client SDK | VMware Horizon package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series). |
| Mozilla_Firefox           | Firefox package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged  |

**Table 5. ThinOS 10 packages (continued)**

| ThinOS 10 packages       | ThinOS image title  |
|--------------------------|---|
|                          | 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).   |
| Microsoft_AVD            | Microsoft AVD package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).        |
| Imprivata_PIE            | Imprivata package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).            |
| Zoom_Universal           | Zoom Universal package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).       |
| Jabra                    | Jabra headsets package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).       |
| Epos_Connect             | EPOS Connect package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).         |
| Cisco_WebEx_VDI          | Cisco Webex VDI package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).      |
| Cisco_WebEx_Meetings_VDI | Cisco Webex Meetings package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series). |
| Cisco_Jabber             | Cisco Jabber package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).         |
| HID_Fingerprint_Reader   | HID Fingerprint Reader package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550,   |

**Table 5. ThinOS 10 packages (continued)**

| ThinOS 10 packages                            | ThinOS image title   |
|---|--|
|   | Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).  |
| Identity_Automation_QwickAccess               | Identity Automation QwickAccess package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series). |
| ControlUp_VDI_Agent                           | ControlUp VDI Agent package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).             |
| RingCentral_App_VMware_Plugin                 | RingCentral App VMware Plugin package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).   |
| Liquidware_Stratusphere_Ux_Connector_ID_Agent | Liquidware package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).                      |
| Lakeside_Virtual_Agent                        | Lakeside Virtual Agent package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).          |
| ThinOS_Telemetry_Dashboard                    | ThinOS Telemetry Dashboard package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).      |
| uxm_Endpoint_Agent                            | uxm Endpoint Agent package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).              |
| eG_VM_Agent                                   | eG VM Agent package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).                     |
| DellDock_WD19_WD22_PFW                        | DellDock_WD19_WD22_PFW <version> for Wyse 5470, OptiPlex 3000 Thin Client, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, and Dell Pro 14 PC14250.  |

**Table 5. ThinOS 10 packages (continued)**

| ThinOS 10 packages | ThinOS image title   |
|--------------------|--|
| U2724DE_PFW        | U2724DE_PFW package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series).   |
| TelegrafAgent      | TelegrafAgent package <version> for Wyse 5070 Thin Client, Wyse 5070 Extended Thin Client, Wyse 5470, Wyse 5470 All-in-One, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, OptiPlex All-In-One 7410, OptiPlex All-in-One 7420, OptiPlex Micro Plus 7010, Latitude 3420, Latitude 3440, Latitude 5440, Latitude 5450, Latitude 5540, Latitude 5550, Dell Pro Rugged 13 RA13250, Dell Pro Rugged 14 RB14250, Dell Pro 16 Plus PB16250, Dell Pro 14 PC14250, Dell Pro 24 All-in-One, and Amulet Hotkey (DX 5 series). |

8. 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](#).

## 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 ThinOS firmware

## Important notes


- You cannot boot into ThinOS if you perform any of the following operations:
  - Disable the onboard network adapter, Trusted Platform Module (TPM), or Platform Trust Technology (PTT).
  - Clear TPM or PTT.
  - Reset BIOS to default factory settings.
- Ensure that the battery is charged to 50% or higher before installing the operating system firmware, application packages, and BIOS firmware.
- If the thin client is registered in Wyse Management Suite group 1 and you set Wyse Management Suite group 2 token in group 1 policy, a dialog box is displayed to change the group. Click **Cancel** to change to group 2 immediately. Alternatively, click **Restart Now** or wait for the 60-second countdown to finish and then reboot to change to group 2.
- If a policy change in a parent or registered child select group includes a new operating system, BIOS, and applications, the device downloads and install them immediately. However, if the policy change occurs in other child select groups, the device downloads and installs the updates.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When manually registering the thin client to Wyse Management Suite manually.
  - When manually turning on the thin client from a turn off state.
  - When manually changing the Wyse Management Suite group.
- When a new firmware or an application notification is displayed on your thin client, click **Next Reboot**:
  - The notification is displayed again if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - If the new firmware or application is published in the same group, the thin client does not download it.
  - The shutdown window asks to **Update and shut down** or **Update and restart** with a yellow dot on their respective icons. ThinOS updates first before shutting down or restarting.

 **NOTE:** After upgrading to ThinOS 10.x 2502 or ThinOS 10.x 2505, all application packages that are released with ThinOS 2411 are deleted. You must install the latest application packages.

## Upgrade ThinOS 9.x to ThinOS 10.x using Wyse Management Suite

### Prerequisites

- Thin client must be running ThinOS version 9.5.3102 or later.
- If you are upgrading from ThinOS 9.5.3102 version or later to ThinOS 10.0052, ensure the following:
  - Sleep mode is disabled.
  - If the system enters sleep mode, send a Wake-on-LAN command through Wyse Management Suite before issuing any real-time commands.

 **NOTE:** Ensure that the Wake-on-LAN option is enabled in the BIOS to use this feature.

- A group with a valid group token must be created in Wyse Management Suite (WMS) to register ThinOS 9.x devices.
- Thin clients must be registered to WMS.
- In cloud environments, ThinOS 10.x application, BIOS, and firmware packages are available in the **Operator Cloud** and **Tenant Cloud**.
- In on-premises environments, manually copy ThinOS 9.x and 10.x firmware and application upgrade packages to the local repository. For more details, see [Support for ThinOS 10.x package management](#).

- Use the appropriate upgrade package (for example, `Root_2505.10_00xx_signed.pkg` or `RootOS_2505_10.00xx_T10.pkg`) to install the base OS. Selected packages are automatically installed after the upgrade.
- Existing policy configurations for ThinOS 9.x can remain active until new configurations are created for the ThinOS 10.x group.

### Steps

1. Log in to **Wyse Management Suite**.
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_2502.10_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. 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 thin client 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.



## Upload and push ThinOS application packages

ThinOS application packages must be installed on the thin client system to use the respective applications.

### Prerequisites

- Create a group in Wyse Management Suite with a group token.
- Register the thin client to Wyse Management Suite.

### 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 **INSTALL**. 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 application packages are not predefined yet. However, setting the **UNINSTALL** option for this category is not permitted. Once you have the application packages in the **Other** category, it is recommended you upgrade the Wyse Management Suite configUI. The new Wyse Management Suite configUI sets the application packages in the new category.

## Download ThinOS 10 ISO image

### About this task

The following devices require an ISO image for ThinOS installation using a USB drive and the Dell OS Recovery Tool. The ISO image is downloaded as a ZIP file and must be extracted before use.

**Table 6. Platforms require ISO image for ThinOS 10 installation**

| Platforms        | Model   |
|------------------|---|
| Thin Clients     | <ul style="list-style-type: none"><li>Wyse 5070 Thin Client</li><li>Wyse 5070 Extended Thin Client</li><li>Wyse 5470</li><li>Wyse 5470 All-in-One</li></ul>   |
| OptiPlex         | <ul style="list-style-type: none"><li>OptiPlex 3000 Thin Client</li><li>OptiPlex 5400 All-in-One</li><li>OptiPlex All-In-One 7410</li><li>OptiPlex All-in-One 7420</li><li>OptiPlex Micro Plus 7010</li></ul> |
| Latitude devices | <ul style="list-style-type: none"><li>Latitude 3420</li><li>Latitude 3440</li><li>Latitude 5440</li><li>Latitude 5450</li><li>Latitude 5540</li><li>Latitude 5550</li></ul>                                   |
| Dell Pro series  | <ul style="list-style-type: none"><li>Dell Pro Rugged 13 RA13250</li><li>Dell Pro Rugged 14 RB14250</li><li>Dell Pro 16 Plus PB16250</li><li>Dell Pro 14 PC14250</li><li>Dell Pro 24 All-in-One</li></ul>     |

To download the ISO image, do the following:


### Steps

1. Go to [Support | Dell](#).
2. In the **Identify a product or ask support search box**, enter a product identifier, for example, **Wyse 5470 Mobile Thin Client** or **Latitude 3440** and click **Search**.  
A list of matching products is displayed.
3. Select the product from the search results to load the product page.
4. On the product support page, click **Drivers & Downloads**.
5. Select the **Operating System** as **ThinOS 10**.
6. Select the **Download Type** as **Operating Systems**.
7. 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.

8. 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 recovery image. Use the same image for recovery/offline USB imaging.

# Install ThinOS from USB drive using Dell OS Recovery Tool

## About this task

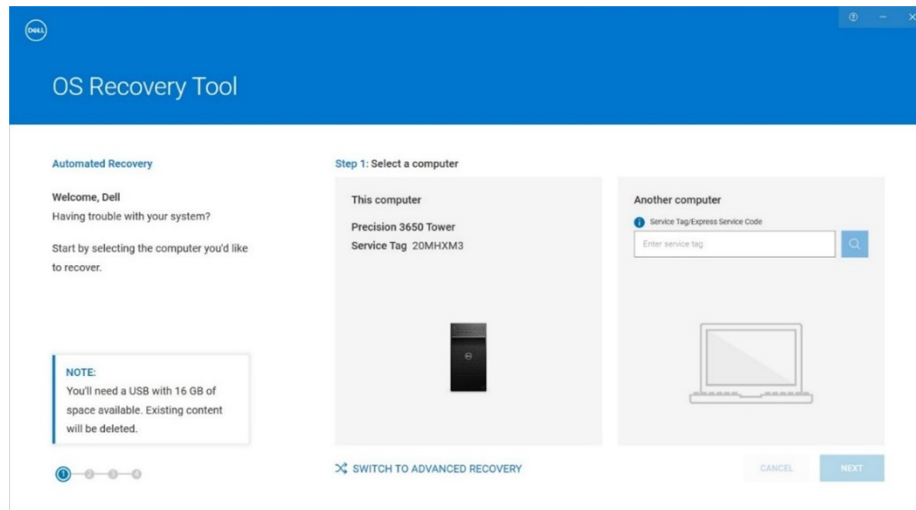
You can install ThinOS from a USB drive using the Dell OS Recovery Tool on the following platforms:

**Table 7. Install ThinOS from a USB drive using the Dell OS Recovery Tool**

| Supported platforms | Model   |
|---------------------|---|
| Thin Clients        | <ul style="list-style-type: none"><li>• Wyse 5070 Thin Client</li><li>• Wyse 5070 Extended Thin Client</li><li>• Wyse 5470</li><li>• Wyse 5470 All-in-One</li></ul>   |
| OptiPlex            | <ul style="list-style-type: none"><li>• OptiPlex 3000 Thin Client</li><li>• OptiPlex 5400 All-in-One</li><li>• OptiPlex All-In-One 7410</li><li>• OptiPlex All-in-One 7420</li><li>• OptiPlex Micro Plus 7010</li></ul> |
| Latitude devices    | <ul style="list-style-type: none"><li>• Latitude 3420</li><li>• Latitude 3440</li><li>• Latitude 5440</li><li>• Latitude 5450</li><li>• Latitude 5540</li><li>• Latitude 5550</li></ul>                                 |
| Dell Pro series     | <ul style="list-style-type: none"><li>• Dell Pro Rugged 13 RA13250</li><li>• Dell Pro Rugged 14 RB14250</li><li>• Dell Pro 16 Plus PB16250</li><li>• Dell Pro 14 PC14250</li><li>• Dell Pro 24 All-in-One</li></ul>     |
| Non-Dell platform   | Amulet Hotkey (DX 5 series)   |

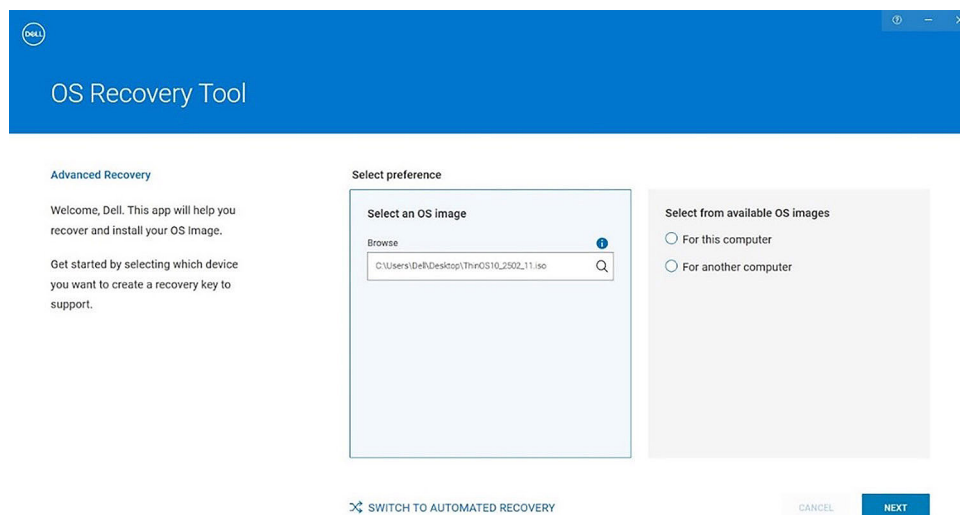
## Steps

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



**Figure 1. Dell OS Recovery Tool**

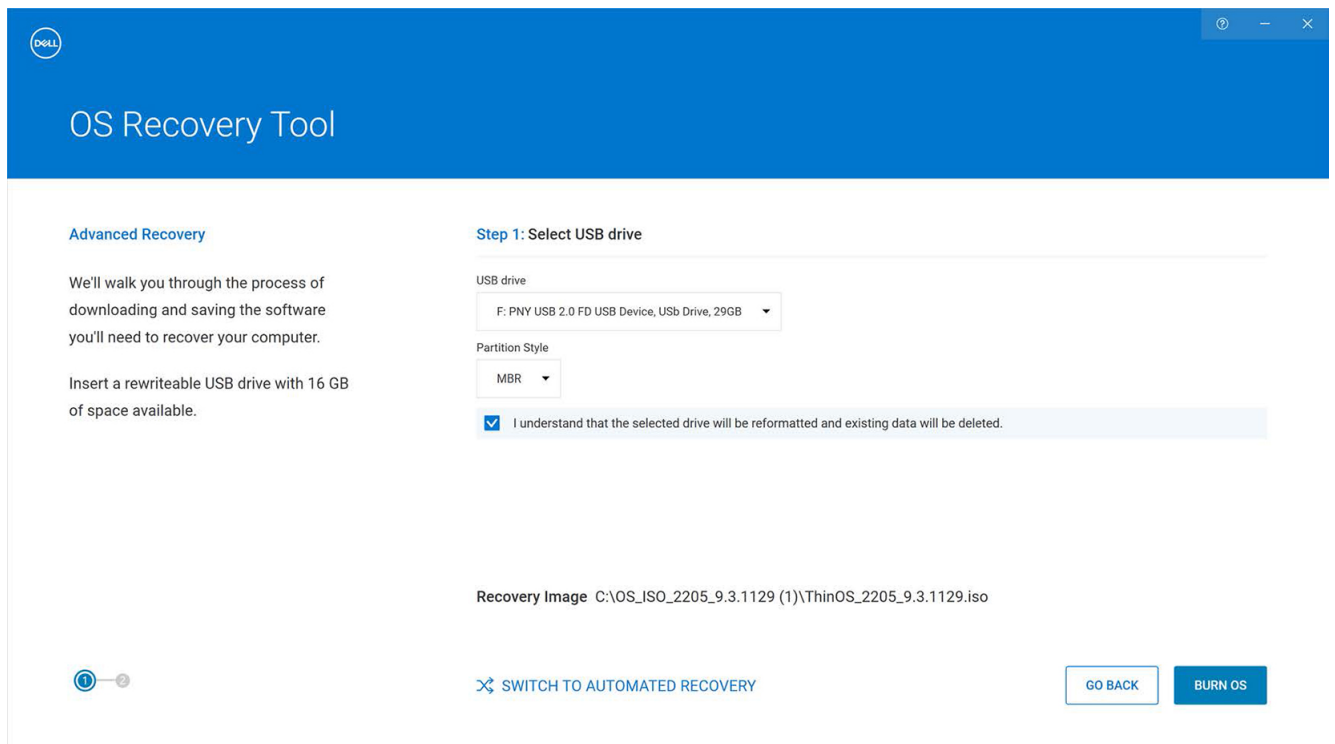
6. In **Select an OS image**, browse to the ISO file that you downloaded in the [Download ThinOS ISO image](#) section and click **NEXT**.



**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.

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

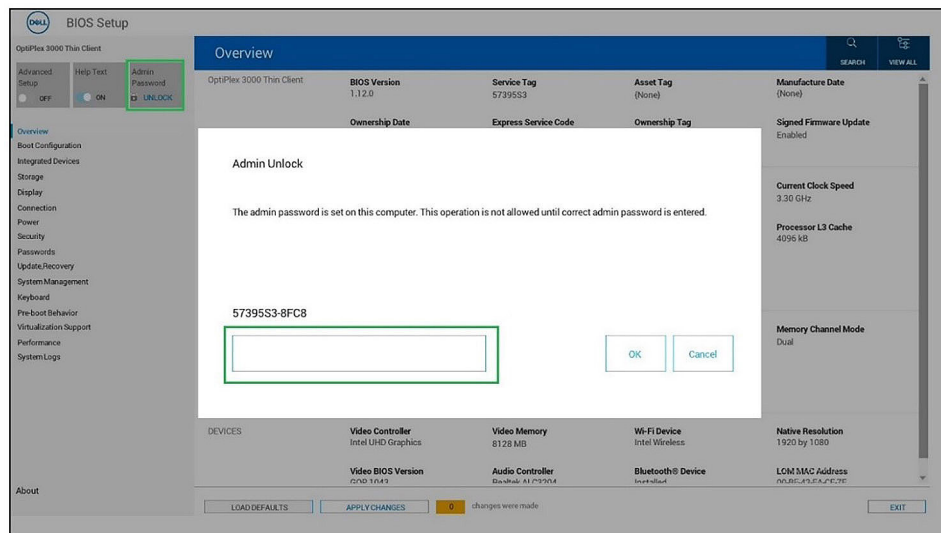


**Figure 3. Burn OS**

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.

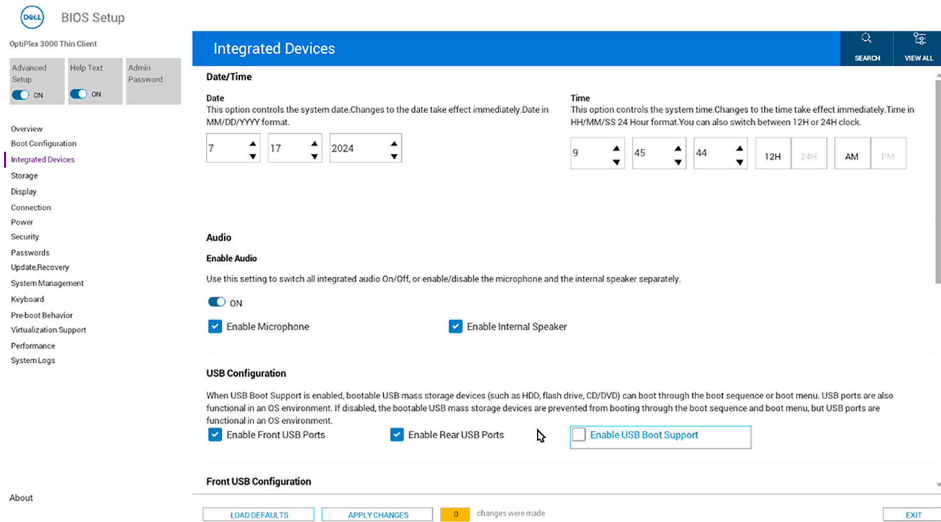
**NOTE:** Once the burn OS process is completed, the build is stored in the USB drive. After the USB drive is removed, Dell OS Recovery Tool goes back to the screen that is displayed in Step 5.

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) .



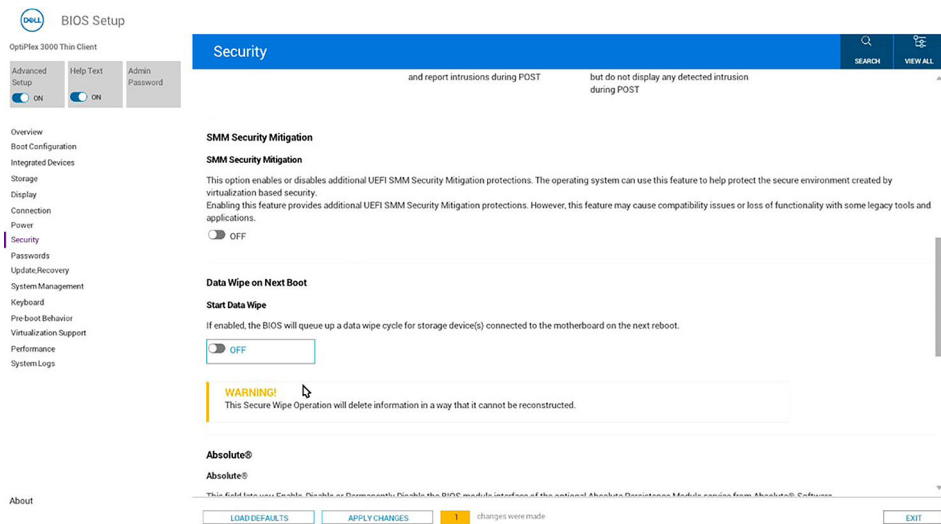
**Figure 4. Unlock BIOS Screen**

13. Click **OK**.  
**NOTE:** The password is case sensitive and after unlocking successfully, the **Admin Unlock** dialog box closes.
14. Go to the **Integrated Devices** section in **BIOS Setup**.
15. Select the **Enable USB Boot Support** checkbox.



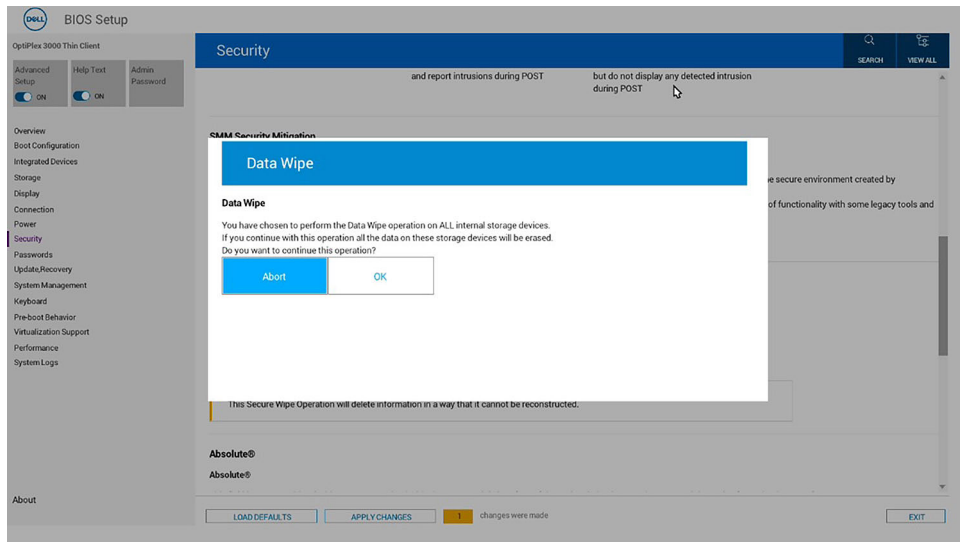
**Figure 5. Enable USB Boot Support**

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



**Figure 6. Data Wipe Screen**

18. A **Data Wipe** dialog box is displayed to confirm the change. Click **OK** to continue the data wipe process.

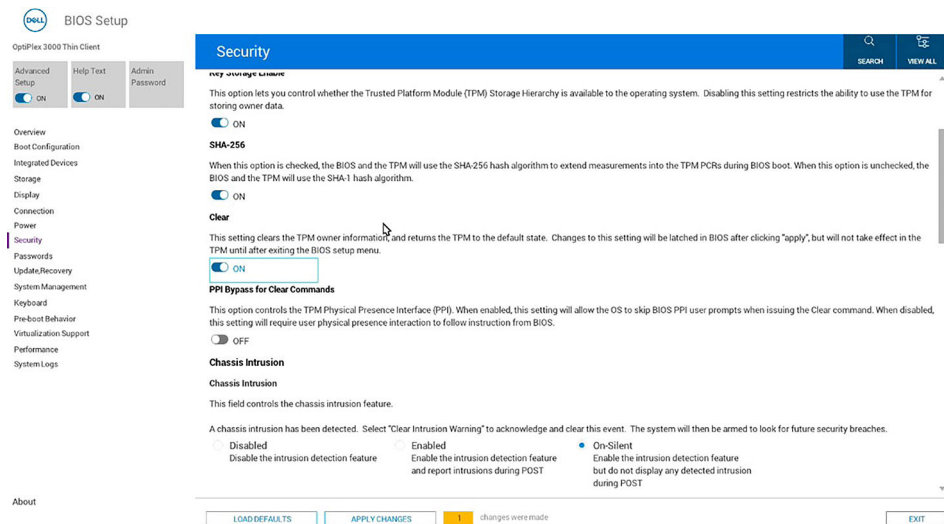


**Figure 7. Data Wipe Screen (Select OK)**

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

19. Click **No**.

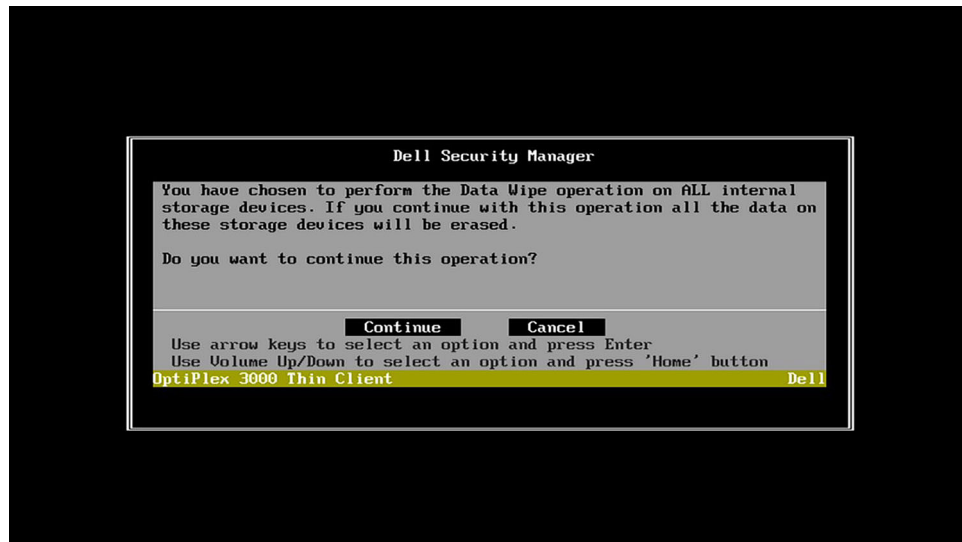
20. Scroll down and enable the **Clear** setting in the **Security** section to clear the user information. A **Clear TPM** dialog box is displayed to confirm the change.



**Figure 8. Clear TPM**

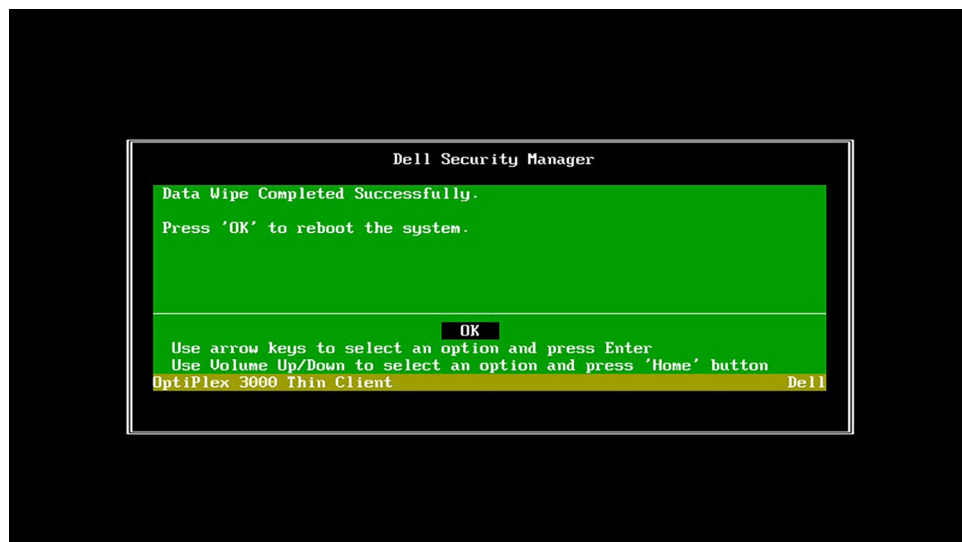
21. Click **Yes**.

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



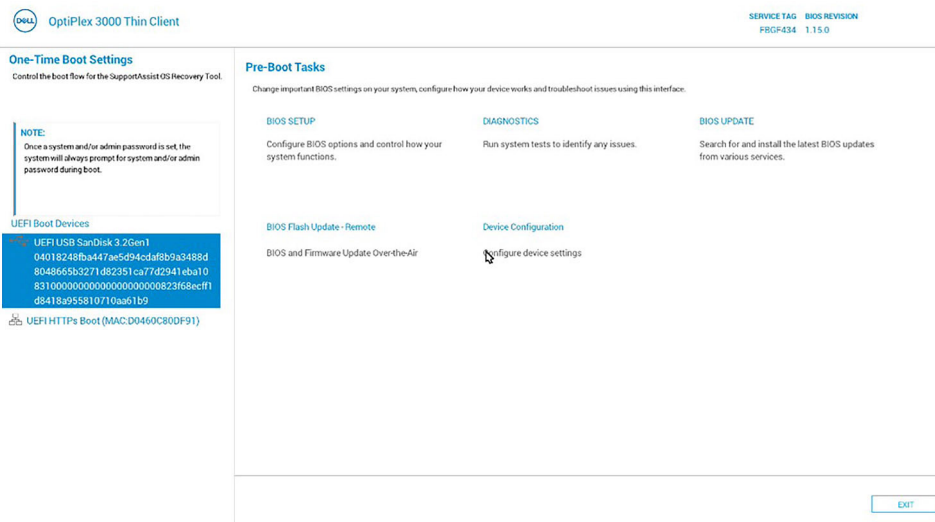
**Figure 9. Dell Security Manager Screen (Select continue)**

23. Click **Continue**.
24. Click **Erase**.  
The data wipe process is complete.
25. Click **OK** to reboot the device.



**Figure 10. Dell Security Manager Screen (Select OK)**

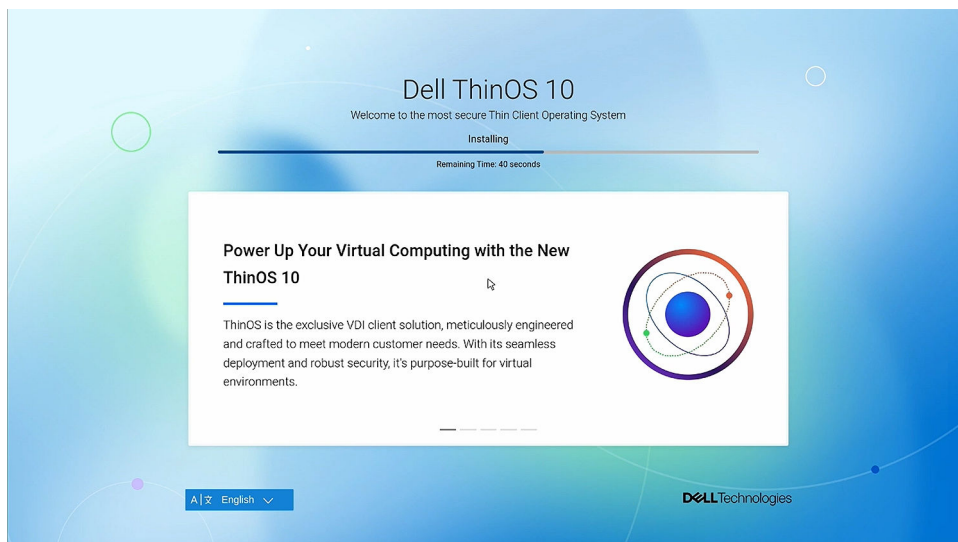
26. Press F12 at boot up until you see the Dell logo and **Preparing one-time boot menu...** displayed at the top, right corner.  
The BIOS boot menu opens.
27. In the boot menu, select the USB drive from the **UEFI Boot Devices** list.



**Figure 11. UEFI Boot Devices USB (Select)**

28. Exit **BIOS**.

Your device automatically reboots, and installation begins. After installation, the OOB screen is displayed.



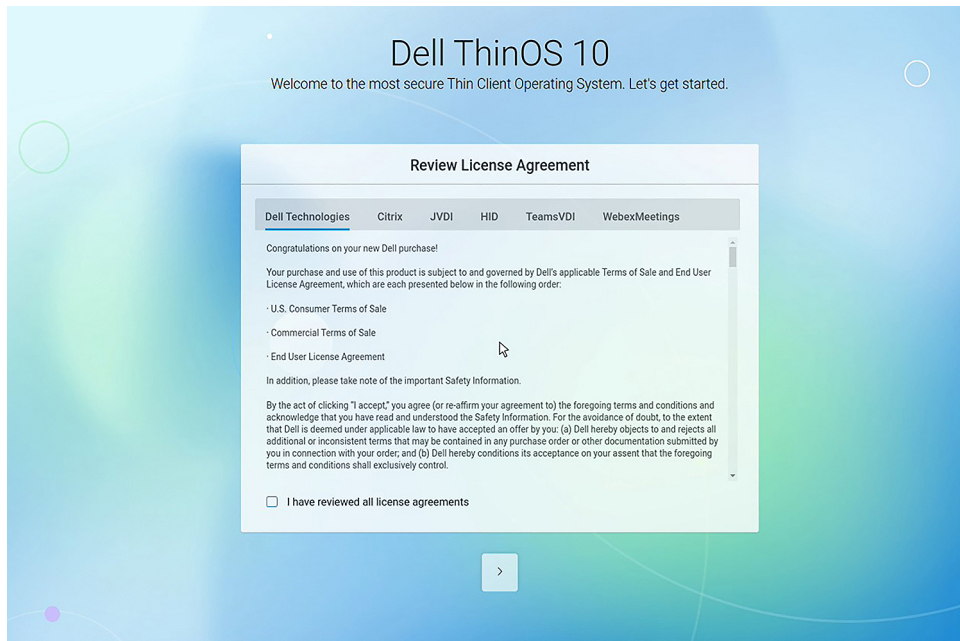
**Figure 12. Installation Screen**

29. 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.

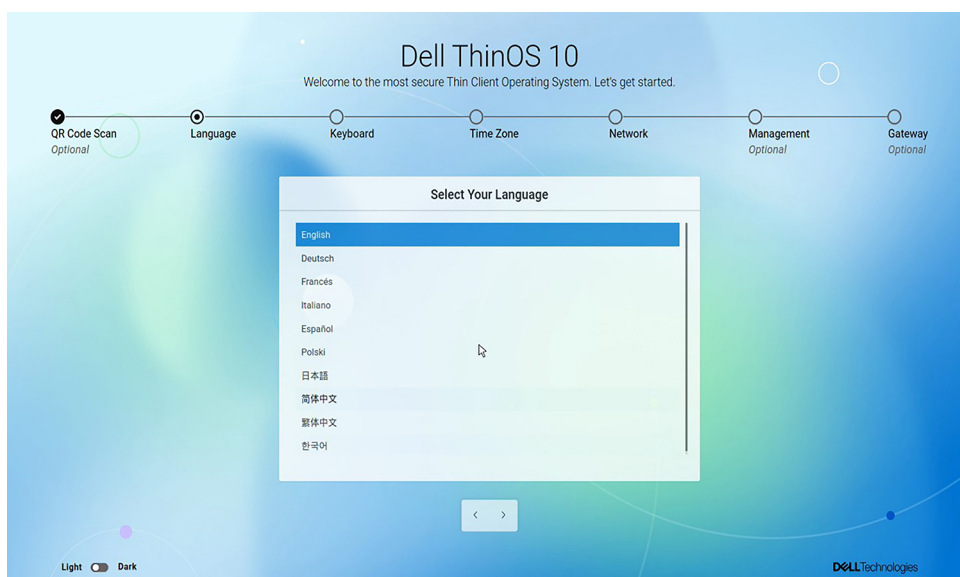
30. In the **Review License Agreement** page, select **Accept All**.





**Figure 13. OOB Screen**

31. 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)**

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



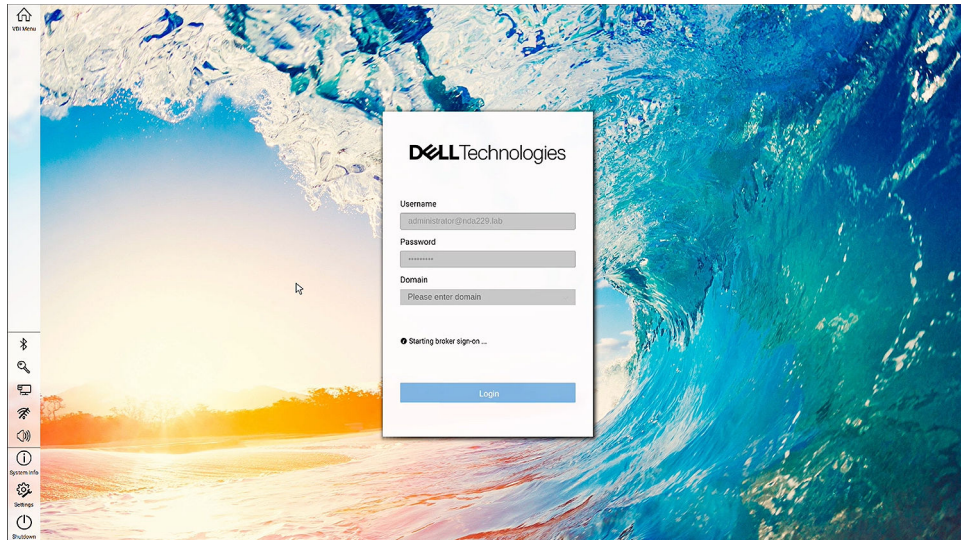


Figure 15. Desktop Screen

## Install ThinOS from USB drive for non-Dell platform

You can install ThinOS from a USB drive for a non-Dell platform.

1. Connect the USB drive to the device.
2. Turn on the device.
3. During boot, press **F10** or **F12** to access the boot menu.
4. From the boot menu, select the connected USB drive as the boot device.

# Register Ubuntu + DCA as Generic Client to Wyse Management Suite

You can register Ubuntu + DCA as a generic client to Wyse Management Suite manually or by using DHCP option tags or DNS SRV records.

## Register Ubuntu + DCA as Generic Client to Wyse Management Suite manually

- Create a group in Wyse Management Suite with a group token.
- The device must be pre-installed with DCA enabler version 2.1.0-271 or later:
  - Open DCA Enabler.
  - Enter the WMS Server and Group Token.
  - Enable or disable CA Validation based on your Wyse Management Suite server license type.
  - Click **Register**.

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

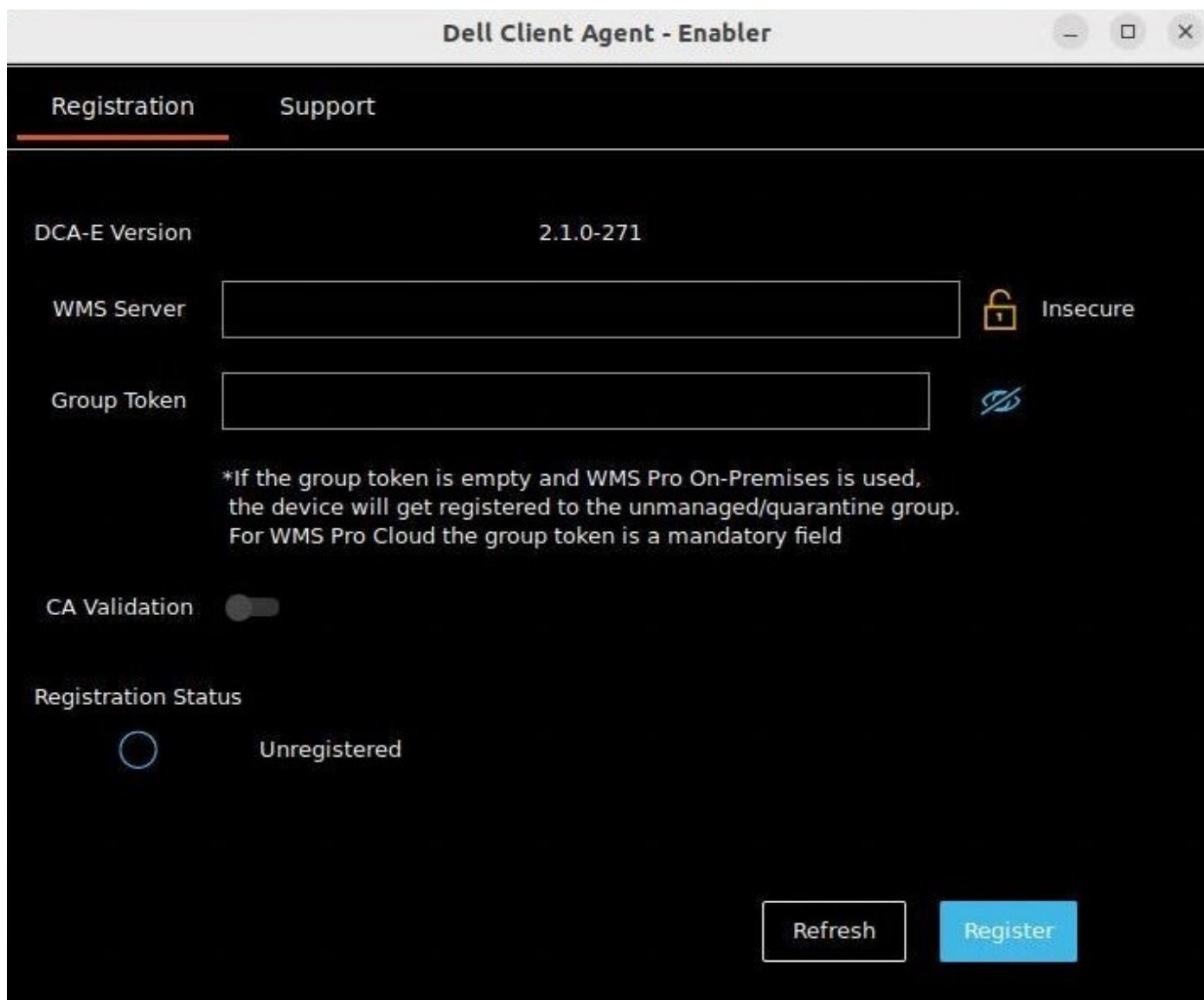


Figure 16. Dell Client Agent - Enabler

## Register Ubuntu + DCA as Generic Client by using DHCP option tags or DNS SRV records

- Ensure that DCA-Enabler 2.1.0-271 or later versions are installed on Ubuntu.
- Create a group in Wyse Management Suite 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 [Wyse Management Suite Environment 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.

# Wyse Management Suite Environment with DHCP and DNS Auto Discovery

ThinOS automated deployment features allow the creation of environments where units can be connected to your network. When connected, they receive the necessary configurations and software updates that are defined by your management software or file servers. Wyse Management Suite automates the deployment of ThinOS thin client devices by configuring the following environmental settings:

**NOTE:** DHCP and DNS SRV configurations for Wyse Management Suite can only function if your device is not already registered.

**NOTE:** If both Wyse Management Suite server and secure Wyse Management Suite server are set, the secure Wyse Management Suite 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 8. DHCP and DNS configuration for Wyse Management Suite**

| Environment                                  | Definition  | IPv4 DHCP User-Defined Option | IPv6 DHCP User-Defined Option | DNS Resource Record      |
|--|---|-------------------------------|-------------------------------|--------------------------|
| Wyse Management Suite Server                 | Specifies the Wyse Management Suite server.   | Option 165 (String)           | Option 16500 (String)         | _WMS_MGMT (SRV)          |
| Wyse Management Suite Server                 | Specifies the secure Wyse Management Suite server.  | Option 201 (String)           | Option 20100 (String)         | _WMS_MGMTV2 (Text)       |
| Wyse Management Suite MQTT Server (optional) | Specifies the MQTT server.  | Option 166 (String)           | N/A                           | _WMS_MQTT (SRV)          |
| Wyse Management Suite CA Validation          | Specifies whether the CA validation is required when you import certificates into your Wyse Management Suite server.  | Option 167 (String)           | Option 16700 (String)         | _WMS_CAVALIDATION (Text) |
| Wyse Management Suite Group Token            | Specifies a unique key that is used by Wyse Management Suite 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)   |
| Wyse Management Suite Group Token            | Specifies a secure unique key that is used by Wyse Management Suite to associate the ThinOS client to the device group Policy.  | Option 202 (String)           | Option 20200 (String)         | _WMS_GROUPTOKENV2 (Text) |

**NOTE:** Dell Technologies recommends 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 Wyse Management Suite.

# Register ThinOS 10.x devices with IPv4 DHCP option tags

You can register the devices by using the following DHCP option tags:

**Table 9. Registering device with IPv4 DHCP option tags**

| Option Tag   | Description  |
|--|--|
| <ul style="list-style-type: none"> <li>Name—WMS</li> <li>Data Type—String</li> <li>Code—201</li> <li>Description—WMS Server FQDN</li> </ul>                                  | <p>This tag directs the device to the URL of the Wyse Management Suite server.</p> <p>For example, <code>wmsserver.acme.com</code>, where <code>wmsserver.acme.com</code> is the fully qualified domain name of the server hosting the Wyse Management Suite.</p> <p><b>NOTE:</b> HTTPS:// is not required in the Wyse Management Suite URL.</p>   |
| <ul style="list-style-type: none"> <li>Name—WMS</li> <li>Data Type—String</li> <li>Code—201</li> <li>Description—Secure WMS Server</li> </ul>                                | <p>This tag directs the device to the Wyse Management Suite server.</p>  |
| <ul style="list-style-type: none"> <li>Name—MQTT</li> <li>Data Type—String</li> <li>Code—166</li> <li>Description—MQTT Server</li> </ul>                                     | <p>This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite 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><b>NOTE:</b> MQTT is optional for Wyse Management Suite 5.0 or later versions.</p>  |
| <ul style="list-style-type: none"> <li>Name—CA Validation</li> <li>Data Type—String</li> <li>Code—167</li> <li>Description—Certificate Authority Validation</li> </ul>       | <ul style="list-style-type: none"> <li>You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud.</li> <li>Enter <b>True</b>, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.</li> <li>Enter <b>False</b>, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.</li> </ul> <p><b>NOTE:</b> CA Validation is optional for Wyse Management Suite 5.0 or later versions. However, it is recommended to configure this option tag.</p>   |
| <ul style="list-style-type: none"> <li>Name—Group Registration Key</li> <li>Data Type—String</li> <li>Code—199</li> <li>Description—Group Registration Key</li> </ul>        | <p>The tag directs the device to retrieve the Group Registration Key for Wyse Management Suite. 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><b>NOTE:</b> Group Token is optional for Wyse Management Suite 5.0 on prem-server. However, there is a known issue that if you do not provide the group token, the device is not moved to an unmanaged group. Therefore, It is recommended to configure the Group Token key.</p> |
| <ul style="list-style-type: none"> <li>Name—Group Registration Key</li> <li>Data Type—String</li> <li>Code—202</li> <li>Description—Secure Group Registration Key</li> </ul> | <p>The tag directs the device to retrieve the secure Group Registration Key for Wyse Management Suite.</p>   |

To get the secure Wyse Management Suite server and secure Group Registration Key, do the following:

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

**NOTE:** Do not set predefined string values for DHCP option tags 201 and 202, as these predefined values are limited to 255 characters. The secure Wyse Management Suite server and secure Group Registration Key can accommodate more than 255 characters. Instead, manually copy and set the secure Wyse Management Suite server and secure Group Registration Key for DHCP option tags 201 and 202.

## WMS auto discovery by IPv6 DHCP option

ThinOS 10.x 2502 supports WMS auto discovery by IPv6 DHCP option. The IPv6 DHCP option tags for WMS auto discovery are listed below:

**Table 10. WMS auto discovery by IPv6 DHCP option**

| Option Tag   | Description   |
|--|---|
| <ul style="list-style-type: none"> <li>Name—WMS</li> <li>Data Type—String</li> <li>Code—16500</li> <li>Description—WMS Server FQDN</li> </ul>                                  | <p>This tag specifies the Wyse Management Suite server URL, such as <code>wmserver.acme.com</code>, where <code>wmserver.acme.com</code> is the fully qualified domain name of the server hosting the Wyse Management Suite.</p> <p><b>NOTE:</b> The <code>HTTPS://</code> prefix is not required in the Wyse Management Suite URL.</p>   |
| <ul style="list-style-type: none"> <li>Name—WMS</li> <li>Data Type—String</li> <li>Code—20100</li> <li>Description—Secure WMS Server</li> </ul>                                | <p>This tag specifies the secure Wyse Management Suite server.</p>  |
| <ul style="list-style-type: none"> <li>Name—CA Validation</li> <li>Data Type—String</li> <li>Code—16700</li> <li>Description—Certificate Authority Validation</li> </ul>       | <ul style="list-style-type: none"> <li>You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud.</li> <li>Enter <b>True</b>, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.</li> <li>Enter <b>False</b>, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.</li> </ul> <p><b>NOTE:</b> CA Validation is optional for Wyse Management Suite 5.0 or later versions. However, it is recommended to configure this option tag.</p>  |
| <ul style="list-style-type: none"> <li>Name—Group Registration Key</li> <li>Data Type—String</li> <li>Code—19900</li> <li>Description—Group Registration Key</li> </ul>        | <p>The tag directs the device to retrieve the Group Registration Key for Wyse Management Suite. 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><b>NOTE:</b> Group Token is optional for Wyse Management Suite 5.0 on prem-server. However, due to a known issue, if you do not provide the Group Token, the device is not moved to an unmanaged group. It is recommended to configure the Group Token key.</p> |
| <ul style="list-style-type: none"> <li>Name—Group Registration Key</li> <li>Data Type—String</li> <li>Code—20200</li> <li>Description—Secure Group Registration Key</li> </ul> | <p>The tag directs the device to retrieve the secure Group Registration Key for Wyse Management Suite.</p>  |

**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

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

**Table 11. 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 Wyse Management Suite URL. For example, wmsserver.acme.com, where wmsserver.acme.com is the qualified domain name of the server.<br><b>NOTE:</b> There is a known issue that https:// is required in the Wyse Management Suite server URL. If you do not use https://, the device cannot automatically check in to Wyse Management Suite.  |
| WMS server (_WMS_MGMTV2, Type Text)                              | This record directs the device to a secure Wyse Management Suite server.   |
| (Optional) WMS MQTT Server                                       | This record directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, wmsservername.domain.com:1883.<br><b>NOTE:</b> MQTT is optional for Wyse Management Suite 5.0 or later versions.  |
| WMS Group Token (_WMS_GROUPTOKEN, Type Text)                     | This record is required to register the ThinOS device with Wyse Management Suite on public or private cloud.<br><b>NOTE:</b> Group Token is case-sensitive. However, it is optional for Wyse Management Suite 5.0 on prem-server.  |
| WMS Group Token (_WMS_GROUPTOKENV2, Type Text)                   | This record directs the device to secure Group Registration Key for Wyse Management Suite.   |
| WMS CA Validation (_WMS_CAVALIDATION, Type Text)                 | <ul style="list-style-type: none"><li>You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite 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.</li><li>Enter <b>True</b>, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.</li><li>Enter <b>False</b>, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.</li></ul> <b>NOTE:</b> CA Validation is optional for Wyse Management Suite 5.0 or later versions. |

To get the secure Wyse Management Suite server and secure Group Registration Key, do the following:

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**.





# Register ThinOS 10.x devices using Wyse Device Agent

If you do not use DHCP or DNS as described in the previous section, you can configure the WDA agent directly from the ThinOS GUI. This configuration must be done individually on each thin client.

## Steps

- To access the central configuration settings, do the following:
  - **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.
- Select the **Enable WMS Advanced Settings** check box.
- In the **WMS server** field, enter the Wyse Management Server URL in the format `https://server.domain`.  
This value represents the Wyse Management Suite server from which ThinOS clients are managed and the client configurations are obtained over SSL.
- In the **Group Registration Key** field, enter the group registration key as configured by your Wyse Management Suite administrator for your group. To verify the setup, click **Validate Key**.  
If the key is not validated, verify the group key and Wyse Management Suite 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.
- Enable or disable CA validation based on your license type. For public cloud, select the **Enable CA Validation** check box. For private cloud, select the **Enable CA Validation** check box if you have imported certificates from a well-known certificate authority into your Wyse Management Suite 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** check box. You can install the certificate to the device by using Wyse Management Suite after registration, and then enable the CA validation option.
- Validate the newly added devices enrollment in Wyse Management Suite, 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 *Wyse Management Suite 5.0 Administrator's guide* at [Support | Dell](#).
- Click **Save**.  
The device checks in to the Wyse Management Suite, and the policy settings are applied.



# Converting to ThinOS 10

## Convert Dell Hybrid Client to ThinOS 10

### Prerequisites

- Wyse Management Suite version 5.0 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 Wyse Management Suite.
- 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 Wyse Management Suite with a group token.
- The Dell Hybrid Client devices must be registered to Wyse Management Suite.
- Ensure to download the Dell Hybrid Client to DHC\_Ubuntu\_To\_ThinOS10\_conversion\_2505\_10.0076.tar package conversion image.

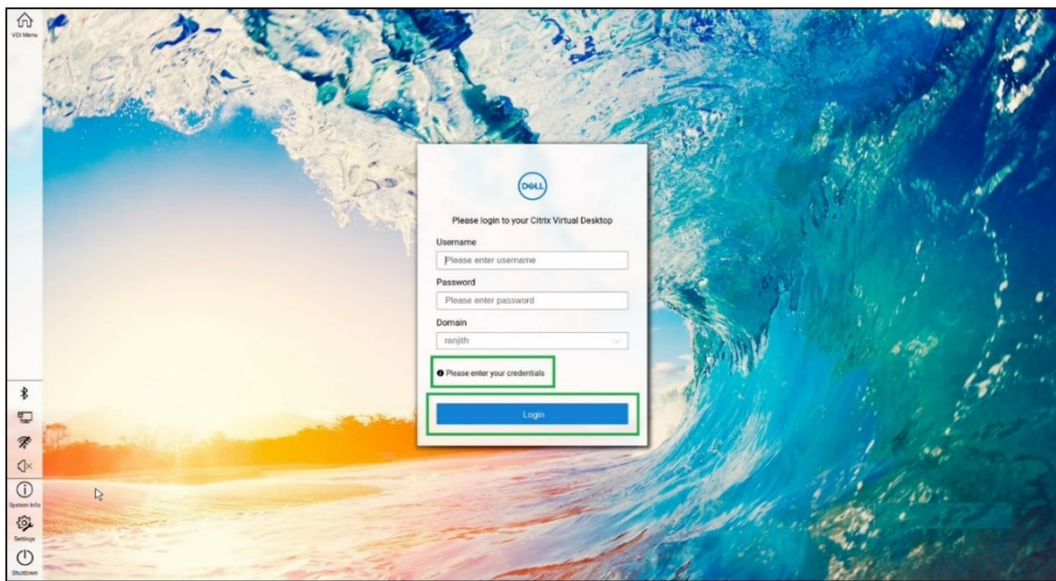
**Table 12. Supported platforms for DHC to ThinOS 10.x**

| Supported platforms for DHC to ThinOS 10.x  |
|---|
| <ul style="list-style-type: none"> <li>• Wyse 5070 Thin Client</li> <li>• Wyse 5070 Extended Thin Client</li> <li>• Latitude 3440</li> <li>• Latitude 5440</li> <li>• Latitude 5450</li> <li>• OptiPlex 3000 Thin Client</li> <li>• OptiPlex 5400 All-in-One</li> <li>• OptiPlex All-In-One 7410</li> <li>• OptiPlex All-in-One 7420</li> <li>• OptiPlex Micro Plus 7010</li> </ul> |

### Steps

1. Log in to **Wyse Management Suite**.
2. Copy DHC\_Ubuntu\_To\_ThinOS10\_conversion\_2505\_10.0076.tar to C:\WMS\LocalRepo\repository\hybridClientApps or follow the steps that are given below:
  - 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\_2505\_10.0076.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\_2505\_10.0076.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 Wyse Management Suite (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 Thin Client device.
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 17. Desktop Screen**

The Desktop screen is displayed.

## Policy configuration

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

## 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 13. Error Log table**

| Error Log        | Resolution                            |
|------------------|---------------------------------------|
| No AC plugged in | Plug in power adapter, reschedule job |

**Table 13. Error Log table (continued)**

| Error Log   | Resolution  |
|---|---|
| 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  |

## Convert systems with Dell Ubuntu for managed clients


### Prerequisites

- Wyse Management Suite version 5.0 is required to convert to ThinOS 10.x.
- Ensure that you have connected the Ubuntu device to the external power source using the power adapter.
- Ensure that you have enough ThinOS 10.x Activation device licenses on Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.
- The number of ThinOS 10.x Activation licenses in Wyse Management Suite must be greater than the number of Dell Ubuntu devices to create the Advanced Policy for conversion.
- The Ubuntu devices must be registered to Wyse Management Suite as generic clients. For details on how to register the generic client to Wyse Management Suite, see [Register Ubuntu + DCA as Generic Client to WMS manually](#).
- Ensure that you have downloaded the DHC\_Ubuntu\_To\_ThinOS10\_conversion\_2505\_10.0076.tar conversion image.

If your device is running the following operating system, ensure that the relevant DCA-Enabler is installed:

**Table 14. Supported conversion scenarios**

| Platform                 | Dell Ubuntu version | DCA-Enabler version |
|--------------------------|---------------------|---------------------|
| Dell Pro 16 Plus PB16250 | 24.04               | 2.1.0-271 or later  |

 **NOTE:** The device must have a factory-installed Ubuntu operating system. Custom installations of Dell Ubuntu are not eligible for conversion to ThinOS 10.x.

### Steps

1. Go to **Apps & Data > App Inventory > Generic Client**, and click **Add Package file**.
2. Upload the Conversion Installer file DHC\_Ubuntu\_To\_ThinOS10\_conversion\_2505\_10.0076.tar
3. Go to **Apps & Data > App Policies > Generic Client**, and click **Add Advanced Policy**.
4. Enter the policy name, select the group in which the Dell Ubuntu device has been registered, and select **Generic Client** as OS type.
5. Click **Add app** and select the previously uploaded ThinOS image file from the drop-down menu.
6. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
7. Select the platforms to convert from the **Platform Filter** drop-down menu.
8. Click **Save**.

 **NOTE:** Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.

9. In the next window, click **Yes** to schedule a job.

10. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.

11. 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 Wyse Management Suite, 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 Wyse Management Suite 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](#).

# Configuring a ThinOS 10.x client using Wyse Management Suite

It is recommended to optimize centralized configuration server groups for better performance and manageability by maximizing the number of unique customer device configuration groups. A minimal number of Wyse Management Suite groups and settings should be used to maximize the unique customer device configurations groups. This is applicable to both multitenant and on-premises scenarios.

When you change the group in Wyse Management Suite, the ThinOS 10.x based thin client displays a message prompting you to restart the thin client immediately or postpone it to the next reboot for applying the latest configurations.

When you deploy a new firmware or package using Wyse Management Suite, the thin client displays a message prompting you to start the installation immediately or postpone it to the next reboot.

## ThinOS 10 configuration grouping overview

During the deployment process, you must evaluate the various needs of your users to determine all the client configurations that are mandatory to meet the requirements. Few configurations such as monitor resolution or VNC password applies to the device, while others such as broker configurations may only apply to specific users of the device.

Redundant configurations may result in performance issues and makes it difficult to manage environmental changes since each device configuration requires to be updated. This issue can be resolved by grouping configurations.

ThinOS 10 configuration grouping determines the parameters inheritance. The child group inherits the settings from its parent group. The following table lists the common device configuration criteria that must be considered when creating groups:

**Table 15. ThinOS 10 configuration grouping overview**

| Group Types                                  | Configurations   |
|--|--|
| Global device configurations                 | <ul style="list-style-type: none"> <li>• Privilege Settings including Admin Mode</li> <li>• Security Policy Settings</li> <li>• Remote Control Settings (VNC)</li> <li>• Management Settings</li> <li>• All other global configurations</li> </ul> |
| Device configurations for a group of clients | <ul style="list-style-type: none"> <li>• Group-based Broker Configurations</li> <li>• Group-based Printer Settings</li> <li>• Group-based Time Zone Settings</li> </ul>  |
| Device configurations for a single device    | <ul style="list-style-type: none"> <li>• Client-based Terminal Name</li> <li>• Client-based Location</li> <li>• Client-based Location and Custom 1, 2, 3</li> </ul>  |
| Device configurations dynamically selected   | ThinOS 10.x Select Group with device configurations  |

## ThinOS 10 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 system variables:

**Table 16. ThinOS 10 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 <b>15</b> .  |
| \$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 unit, including 169, 140, 141, 166, 167. For example, set a string <b>test169</b> for the <b>tag169</b> option in the DHCP server, and set <b>TerminalName=\$DHCP(169)</b> in the Wyse Management Suite policy. Check the terminal name in the UI, and the terminal name is <b>test169. 166</b> and <b>167</b> 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 <b>\$DHCP(166)</b> or <b>\$DHCP(167)</b> .                             |
| \$DN                                | Sign on domain name   |
| \$TN                                | Terminal name   |
| \$UN                                | Sign on username  |
| \$SUBNET                            | For subnet notation, the format is <b>{network_address}_{network_mask_bits}</b> . 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, include=&Left(\$FIP,11).ini 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 <b>\$xx</b> is any of above parameters, and the parameter <b>i</b> 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 <b>\$xx</b> is any of the above System Variables. The option <b>i</b> specifies left or right offset digits. For example, in the parameter <b>TerminalName=CLT-\$SN\$RIGHT\$07</b> , 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: <ul style="list-style-type: none"> <li>• First four characters—CLT-</li> <li>• The rest—The last right-most seven digits of the thin client serial number. The resulting terminal name is displayed as CLT-MA00256.</li> </ul> |
| \$AT                                | <b>Asset Tag</b> must be enabled in the BIOS settings. <b>\$AT</b> can be used as terminal name, and the length is limited to 32 characters.  |

# BIOS Installation

## Upgrade BIOS

### Prerequisites

- Download the BIOS file from [Support | Dell](#) to your device.
- If you are upgrading BIOS using Wyse Management Suite, register the thin client to Wyse Management Suite.

### About this task

- NOTE:** You must upgrade the operating system image first, and then upgrade the BIOS after the operating system image is successfully upgraded. Do not upgrade the BIOS and the operating system image together. If you upgrade the BIOS and the operating system image together, the BIOS upgrade is ignored, and you cannot upgrade the BIOS to the ignored version. You must upgrade the BIOS to another version.

### Steps

1. Open the Admin Policy Tool on the thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
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** drop-down menu, select the BIOS file that you have uploaded.
6. Click **Save & Publish**.

The thin client restarts. BIOS is upgraded on your device.

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

- 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.

## Edit BIOS settings

### Prerequisites






- If you are using Wyse Management Suite, ensure that you have registered the thin client 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](#).

- NOTE:** 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 thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.

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, the new password is applied after the first reboot. Other setting changes are applied after the second reboot.
-  **NOTE:** If you change the BIOS password using a select group, it requires a reboot to take effect.
-  **NOTE:** If you enable **Set Admin Password**, set a new BIOS password and then reboot the thin client, the new BIOS password is synced to the WMS server automatically.
-  **NOTE:** If you first enable **Set Admin Password**, set the new BIOS password, and then disable **Set Admin Password**, the BIOS password is cleared 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.




# Delete ThinOS 10 application packages

You can use the ThinOS local user interface or Wyse Management Suite to delete one or more ThinOS packages.

## Steps

1. Log in to the ThinOS 10 client.
2. From the system menu, go to **System Tools > Packages**.  
All the installed ThinOS 10 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.

For information about how to delete packages using Wyse Management Suite, follow all steps in [Upload and push ThinOS application packages](#), except step six, where you must switch to **UNINSTALL**.

## 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, **Latitude 3440** or **OptiPlex All-In-One 7410** 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**.

## 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.