# Dell Wyse ThinOS 2303, 2211, 2208, and 2205

## Migration Guide

March 2023
Rev. A06

## 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.**

# Contents

# Introduction

This guide contains instructions to migrate from Ubuntu and ThinOS 9.1.3129 or later versions to ThinOS 2205, 2208, 2211, 2303 or later versions using Wyse Management Suite 3.7 or later versions.

The overall migration process includes the following tasks:

1. Register the thin client to the Wyse Management Suite server using the following method:
    - Automate the Wyse Management Suite server and Group Registration Token discovery using the DHCP or DNS records.
2. Download the ThinOS firmware from the www.dell.com/support site—see Download the ThinOS firmware, BIOS, and application packages.
3. Configure the ThinOS 9.x-based device using Wyse Management Suite version 3.7 or later versions—see Configuring a ThinOS 9.x client using Wyse Management Suite.

If you convert a device from another operating system to ThinOS 2303 or install the ThinOS 2303 recovery image, ThinOS changes BIOS settings when booting for the first time:

- BIOS password: Set to **Fireport**
- SATA/NVMe Operation: Set to **AHCI/NVMe**
- Integrated NIC: Set to **Enabled** (set to disable PXE boot support)
- Wake-on-LAN: Set to **LAN only**
- Enable Secure Boot: Set to **ON**
- Enable USB Boot Support: Set to **OFF**
- Enable USB Wake Support: Set to **ON**
- Deep Sleep Control: Set to **Disabled**

    **NOTE:** Only the devices with BIOS password **Fireport** or an empty password field applies these changes in BIOS settings.

**NOTE:** As part of the upcoming ThinOS release, the implementation method of library dependencies for third-party packages is going to change. Third-party packages that are released prior to ThinOS 2205 are going to be uninstalled from your ThinOS device when upgrading to the future ThinOS release.

## Supported platforms

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- OptiPlex 3000 Thin Client
- Latitude 3420
- OptiPlex 5400 All-in-One
- Latitude 3440
- Latitude 5440
- OptiPlex All-in-One 7410

## Supported Wyse Management Suite versions

The following are the supported Wyse Management Suite versions:

- Wyse Management Suite 3.7, 3.8, 4.0 Standard and Pro
- Wyse Management Suite 3.7, 3.8, 4.0

Wyse Management Suite default communications are handled over port 443. Wyse Management Suite server values must be defined in the ThinOS user interface or provided by DHCP or DNS services.

**NOTE:** For information about the Wyse Management Suite Standard download and Pro trial, go to www.dell.com/wyse/wms/trial. For information about Wyse Management Suite manuals, go to the Wyse Management Suite product page at www.dell.com/support.

# Prerequisites before you upgrade to ThinOS 9.x

- If you are using ThinOS 8.6 or earlier versions of ThinOS 9.x, you must upgrade to ThinOS 9.1.3129 or later versions before upgrading to ThinOS 2205, 2208, or later versions. See Dell Wyse ThinOS 9.1.4234, 9.1.5067 and 9.1.6108 Migration Guide at www.dell.com/support
- You can't upgrade from ThinOS 8.6 to ThinOS 2205 or later versions directly due to a firmware image file size limitation.
- Before upgrading from ThinOS 9.x to later versions, ensure that your system is powered on and the sleep mode is disabled on the system. If the system has entered the sleep mode, you must send the Wake-On-LAN command through Wyse Management Suite before using any real-time commands. To use the Wake-On-LAN command, ensure that the Wake-On-LAN option is enabled in BIOS.

## Important notes

- You cannot boot into ThinOS 2205, 2208, or later versions when you perform the following operations:
  - Disable the onboard Network Interface Card (NIC), Trusted Platform Module (TPM), or Platform Trust Technology (PTT).
  - Clear TPM or PTT.
  - Reset BIOS to factory default settings.
- From ThinOS 2208, you must connect the power adapter to install the operating system firmware, application package, 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. Click **Restart Now** or wait for the 60-seconds countdown to finish and then reboot to change to group 2.
- ThinOS 2205 or later versions does not apply operating system firmware application package and BIOS firmware if you switch the child select group in the login window.
- If the **Live Update** option is disabled, the thin client cannot download and install a 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 you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
  - Not display a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - Not display any notification from if the new firmware or application is downloaded in the same group.
  - Install the firmware or package after a reboot.
- The upgrade may fail if the event log fails to install. In such an event, you may reboot the device and upgrade again.
- If you are migrating from a non-ThinOS operating system, such as Ubuntu, a ThinOS Activation License is needed. See Dell Wyse ThinOS Installation and ThinOS Activation License User Guide at www.dell.com/support for more information.

**NOTE:** After upgrading to ThinOS 2205 or later versions, all application packages released before 2205 are removed automatically and cannot be installed again. You must install the latest application packages.

2

# Wyse Management Suite Environment Automation using DHCP and DNS

ThinOS automated deployment features can be used to create environments where units can be attached to your network. It also helps in receiving the required configurations and software updates that are defined by your management software or file servers. Wyse Management Suite automated deployment of ThinOS thin client devices is achieved by configuring the following environmental information:

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

**NOTE:** If you set both WMS server and secure WMS server, secure WMS server takes priority. If you set both unique group token key and secure unique group token key, secure unique group token key takes priority.

**Table 1. DHCP and DNS configuration for Wyse Management Suite**

| Environment | Definition | DHCP User-Defined Option | DNS Resource Record |
|---|---|---|---|
| Wyse Management Suite Server | Specifies the Wyse Management Suite server. | Option 165 (String) | _ WMS_MGMT (SRV) |
| Wyse Management Suite Server | Specifies the secure Wyse Management Suite server. | Option 201 (String)<br>**NOTE:** Supported from ThinOS 9.1.6108, do not set this value if your current version is earlier than 9.1.6108. | _WMS_MGMTV2 (Text)<br>**NOTE:** Supported from ThinOS 9.1.5067, do not set this value if your current version is earlier than 9.1.5067. |
| Wyse Management Suite MQTT Server (optional) | Specifies the MQTT server. | Option 166 (String) | _ 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) | _ 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 desired 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) | _ 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 desired Device Group Policy. | Option 202 (String)<br>**NOTE:** Supported from ThinOS 9.1.6108, do not set this value if your current version is earlier than 9.1.6108. | _WMS_GROUPTOKENV2 (Text)<br>**NOTE:** Supported from ThinOS 9.1.5067, do not set this value if your current version is earlier than 9.1.5067. |

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 devices by using DHCP option tags

**About this task**

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

**Table 2. Registering device by using DHCP option tags**

| Option Tag | Description |
|---|---|
| Name—WMS<br>Data Type—String<br>Code—165<br>Description—WMS Server FQDN | This tag points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com`, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed.<br>ⓘ **NOTE:** HTTPS:// is not required in the Wyse Management Suite URL. |
| Name—WMS<br>Data Type—String<br>Code—201<br>Description— Secure WMS Server | This tag points to the secure Wyse Management Suite server. |
| Name—MQTT<br>Data Type—String<br>Code—166<br>Description—MQTT Server | 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, `wmsservername.domain.com:1883`. WDA automatically fetches the MQTT details when devices check in for the first time.<br>ⓘ **NOTE:** MQTT is optional for Wyse Management Suite 2.0 and later versions. |
| Name—CA Validation<br>Data Type—String<br>Code—167<br>Description—Certificate Authority Validation | You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud.<br>Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.<br>Enter **False**, if you have not imported the SSL certificates from a well-known authority for https com@Wedding2020munication between the client and the Wyse Management Suite server.<br>ⓘ **NOTE:** CA Validation is optional for the latest version of Wyse Management Suite 2.0 and later versions. However, it is recommended to configure this option tag. |
| Name—Group Registration Key<br>Data Type—String<br>Code—199<br>Description—Group Registration Key | The tag directs the device to fetch the Group Registration Key for Wyse Management Suite. For example, in SCDA-DTos91SalesGroup, for the second part of the Group Registration Key, you must use 8-31 characters, with at least 1 upper, 1 lower, 1 number, 1 special character. However, special characters such as \(backslash), "(double quotes), '(single quote) are not allowed. The Group Registration Key is case sensitive.<br>ⓘ **NOTE:** Group Token is optional for Wyse Management Suite 2.0 and later versions on private cloud. However, there is a known issue that if you do not provide the group token, the device is not moved to unmanaged group. Therefore, It is recommended to configure the Group Token key. |
| Name— Group Token<br>Data Type—String<br>Code—202<br>Description— Secure Group Token | The tag directs the device to fetch the secure Group Registration Key for Wyse Management Suite. |

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 list.
4. Click **Generate Details**.

   ⓘ **NOTE:** Do not set predefined string values for DHCP option tag 201 and 202. Predefined values are limited to 255 characters while secure Wyse Management Suite server and secure Group Registration Key can accommodate more than 255 characters. Copy the secure Wyse Management Suite server and secure Group Registration Key and set DHCP option tag 201 and 202 string values manually.

# Configuring devices by using DNS SRV record

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

**Table 3. Configuring devices by using DNS SRV record**

| Option tag | Description |
|---|---|
| WMS server (_WMS_MGMT, Type SRV, Protocol _tcp, Port number 443) | This record points to the Wyse Management Suite server URL. For example, wmsserver.acme.com, where wmsserver.acme.com is the qualified domain name of the server.<br>ⓘ **NOTE:** 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 points to 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>ⓘ **NOTE:** MQTT is optional for Wyse Management Suite 2.0 and 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>ⓘ **NOTE:** Group Token is case sensitive. However, it is optional for Wyse Management Suite 2.0 and later versions on private cloud. |
| WMS Group Token (_WMS_GROUPTOKENV2, Type Text) | This record points to secure Group Registration Key for Wyse Management Suite. |
| WMS CA Validation (_WMS_CAVALIDATION, Type Text) | You can enable or disable 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.<br>Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server.<br>Enter **False**, 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.<br>ⓘ **NOTE:** CA Validation is optional for Wyse Management Suite 2.0 and 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 list.
4. Click **Generate Details**.

3

# Register ThinOS 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 from within the ThinOS GUI. This has to be configured on every thin client.

### Steps

1. From the desktop menu of the thin client, go to **System Setup** > **Central Configuration**.
   The **Central Configuration** window is displayed.

   ⓘ **NOTE:** Privilege must be set to **High** or Admin Mode must be activated to gain access to the ThinOS Central Configuration menu.
2. Select the **Enable WMS Advanced Settings** check box.
3. 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.
4. 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 which you have provided. Ensure that ports mentioned are not blocked by the network. The default ports 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 **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.
6. 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 the manual and auto registration of thin clients to a group.

   When the **Enrollment Validation** option is enabled, the manual or autodiscovered 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 2.0 Administrator's guide* at www.dell.com/support.
7. Click **OK**.
   The device checks in to the Wyse Management Suite and the policy settings are applied.

# Install DCA-Enabler on Ubuntu

You can install DCA-Enabler on Ubuntu devices manually or through Wyse Management Suite.

## Install DCA-Enabler manually on Ubuntu

### Prerequisites

- Download DCA-Enabler 1.5.0-14 or later versions from www.dell.com/support.
- Extract the file **DCA_Enabler_x.x.zip** to get **DCA_Enabler_x.x_amd64_signed.tar.gz** and **DCA_Enabler_Packages_x.x_amd64_signed.tar.gz**
- Extract **DCA_Enabler_x.x_amd64_signed.tar.gz** and **DCA_Enabler_Packages_x.x_amd64_signed.tar.gz** until you get the two files **dca-enabler_x.x_amd64.deb** and **dca-enabler-packages_x.x_amd64.deb**

### Steps

1. Copy the two files to the **Downloads** folder on Ubuntu.
2. Press **Ctrl + Alt + T** on the keyboard to open the terminal window.
3. Run **cd Downloads** to enter the **Downloads** folder in the terminal.
4. Run **sudo dpkg -i dca-enabler-packages_x.x_amd64.deb** and enter the password to install this file first.
5. Run **sudo dpkg -i dca-enabler_x.x_amd64.deb** to install this file next.

   **NOTE:** Edit the DCA version numbers as per your requirement.

## Upgrade DCA-Enabler through WMS on Ubuntu

### Prerequisites

- Download DCA-Enabler 1.5.0-14 or later versions from www.dell.com/support.
- Extract the file **DCA_Enabler_x.x.zip to get DCA_Enabler_x.x_amd64_signed.tar.gz** and **DCA_Enabler_Packages_x.x_amd64_signed.tar.gz**
- Create a group in Wyse Management Suite with a group token.
- The Ubuntu devices must be registered to Wyse Management Suite as generic clients.

### Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the file **DCA_Enabler_Packages_x.x_amd64_signed.tar.gz**.
3. Click **Add Package file** again and upload the file **DCA_Enabler_x.x_amd64_signed.tar.gz**
4. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
5. Enter the policy name, select the group in which Ubuntu 20.04 has been registered, and select **Generic Client** as OS type.
6. Click **Add app**, and select the file **DCA_Enabler_Packages_x.x_amd64_signed.tar.gz** that was uploaded before from the drop-down menu.
7. Click **Add app** again, and select the file **DCA_Enabler_x.x_amd64_signed.tar.gz** that was uploaded before from the drop-down menu.
8. Click **Save**.
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 DCA-Enabler files download and install on Ubuntu 20.04 devices. You can check the job status from the Wyse Management Suite server Jobs page.

# 5

# 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 WMS manually

### Prerequisites

- Create a group in Wyse Management Suite with a group token.
- If you have installed DCA enabler version 1.7.0-20 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**.
- If you have installed DCA enabler version 1.5.0-14 or 1.6.0-9:
  - Log in to the Wyse Management Suite server.
  - Go to the **Portal Administration** tab.
  - Under **Console Settings** > **Generic Client Registration**, locate your Wyse Management Suite group name.
  - According to your Wyse Management Suite settings, click **Bootstrap** or **Bootstrap-HTTPS-no-CA-validation** to download the configuration file.
  - Rename the file to **reg.json**.
    - If you do not have access to the Wyse Management Suite console, you can create the file using this syntax. Replace the highlighted content with values for your environment:

      ```
      {"ccm":
      {"ccmserver":"fqdn.of.your.wms.server","ccmport":"443","usessl":"true","mqttserver":"fq
      dn.of.your.mqtt.server","mqttport":"1883","grouptoken":"your.WMS.GroupToken"  ,"isCaV
      alidationOn":"false/true"} }}
      ```

    - Keep the syntax in lower case except as needed for the Wyse Management Suite group token.
    - There is no hyphen between the group prefix and group key.
  - Log in to the Ubuntu device.
  - Copy the **reg.json** file to the Ubuntu device.
  - Open a terminal session and go to the directory where the **reg.json** file is located.
  - Run the following command:

    -
      ```
      sudo cp reg.json /etc/dcae/config <Enter>
      ```
  - Restart the DCA enabler, open a terminal session, and enter the following command:

    -
      ```
      sudo systemctl restart dcae.service <Enter>
      ```
  - The device attempts to register with the Wyse Management Suite server and after registration, the device is listed as **Type = Generic Client**

### Steps

1. Create a .txt file and enter the following:

```
{
  "ccm": {
    "ccmserver": "WMS server",
```

```
    "ccmport": "443",
    "usessl": "true",
    "mqttserver": "",
    "mqttport": "1883",
    "grouptoken": "WMS group token",
    "isCaValidationOn": "true or false according to your WMS server setting"
  }
}
```

- Here is an example with Wyse Management Suite server **us1.wysemanagementsuite.com**, group token **thin-Ubuntu20.04** and CA validation **true**

  ```
  {
    "ccm": {
      "ccmserver": "us1.wysemanagementsuite.com",
      "ccmport": "443",
      "usessl": "true",
      "mqttserver": "",
      "mqttport": "1883",
      "grouptoken": "thin-Ubuntu20.04",
      "isCaValidationOn": "true"
    }
  }
  ```

2. Save the .txt file and rename it to **reg.json**

   **NOTE:** The file name is **reg** and the file extension is **json**.

3. Copy the file to the **Downloads** folder on Ubuntu 20.04.
4. Press **Ctrl + Alt + T** on the keyboard to open the terminal window.
5. Run **cd Downloads** to enter the **Downloads** folder in the terminal.
6. Run **sudo cp reg.json /etc/dcae/config** and enter the password to copy this file to the **/etc/dcae/config** folder.
7. Reboot the Ubuntu 20.04 device.
   The device is registered to the Wyse Management Suite server.

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

### Prerequisites

- Ensure that DCA-Enabler 1.5.0-14 or later versions is installed on Ubuntu 20.04.
- 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 section.

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

6

# Download the ThinOS firmware, BIOS, and application packages

This section describes the steps to download the ThinOS firmware from Dell support site.

**Steps**

1. Go to the www.dell.com/support site.
2. Locate the required ThinOS Image entry and click the download icon.

**Table 4. ThinOS 2303 image**

| Scenario | ThinOS image title |
|---|---|
| Upgrade your ThinOS 9.1.3129 or later versions to 2303 (9.4.1141) | ThinOS 9.1.3129 or later to ThinOS 2303 (9.4.1141) Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, Dell OptiPlex 3000 Thin Client, Dell Latitude 3420, 3440, and 5440, Dell OptiPlex 5400 All-in-One with ThinOS, and Dell OptiPlex 7410 All-in-One |
| Ubuntu to ThinOS 2303 conversion image | ThinOS 2303 Ubuntu conversion image for Latitude 3420 and OptiPlex 5400 All-in-One. |

**Table 5. ThinOS 2211 image**

| Scenario | ThinOS image title |
|---|---|
| Upgrade your ThinOS 9.1.3129 or later versions to 2211 (9.3.3096) | ThinOS 9.1.3129 or later to ThinOS 2211 (9.3.3096) Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, Dell OptiPlex 3000 Thin Client, Dell Latitude 3420 with ThinOS, and Dell OptiPlex 5400 All-in-One with ThinOS |
| Ubuntu to ThinOS 2211 conversion image | ThinOS 2211 Ubuntu conversion image for Latitude 3420 and OptiPlex 5400 All-in-One. |
| WES to ThinOS 2211 conversion image | ThinOS 2211 WES conversion image for Wyse 5070 Thin Client, Wyse 5470 Mobile Thin Client, and Wyse 5470 All-in-One Thin Client. |

**Table 6. ThinOS 2208 image**

| Scenario | ThinOS image title |
|---|---|
| Upgrade your ThinOS 9.1.3129 or later versions to 2208 (9.3.2102) | ThinOS 9.1.3129 or later to ThinOS 2208 (9.3.2102) Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, Dell OptiPlex 3000 Thin Client, and Dell Latitude 3420 with ThinOS |
| Ubuntu to ThinOS 2208 conversion image | ThinOS 2208 conversion image for Latitude 3420 and OptiPlex 5400 All-in-One. |

**Table 7. ThinOS 2205 image**

| Scenario | ThinOS image title |
|---|---|
| Upgrade your ThinOS 9.1.3129 or later versions to 2205 (9.3.1129) | ThinOS 9.1.3129 or later to ThinOS 2205 (9.3.1129) Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, and Dell OptiPlex 3000 Thin Client |

3. If you want to use ThinOS packages, locate a package and click the download icon.

**Table 8. ThinOS packages**

| ThinOS packages | ThinOS image title |
|---|---|
| Citrix_Workspace_App | ThinOS YYMM <version> Citrix package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| VMware_Horizon | ThinOS YYMM <version> VMware Horizon package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Teradici_PCoIP | ThinOS YYMM <version> Teradici PCoIP package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Microsoft_AVD | ThinOS YYMM <version> Microsoft AVD package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Imprivata_PIE | ThinOS YYMM <version> Imprivata package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Zoom_Horizon | ThinOS YYMM <version> Zoom Horizon package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Zoom_Citrix | ThinOS YYMM <version> Zoom Citrix package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Jabra | ThinOS YYMM <version> Jabra headsets package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| EPOS_Connect | ThinOS YYMM <version> EPOS Connect package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Cisco_WebEx_VDI | ThinOS YYMM <version> Cisco Webex VDI package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Cisco_WebEx_Meetings | ThinOS YYMM <version> Cisco Webex Meetings package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Cisco_Jabber | ThinOS YYMM <version> Cisco Jabber package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| HID_Fingerprint_Reader | ThinOS YYMM <version> HID Fingerprint Reader package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Identity_Automation_QwickAccess | ThinOS YYMM <version> Identity Automation QwickAccess package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Zoom_AVD | ThinOS YYMM <version> Identity Automation QwickAccess package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| ControlUp_VDI_Agent | ThinOS YYMM <version> ControlUp VDI Agent package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |

**Table 8. ThinOS packages (continued)**

| ThinOS packages | ThinOS image title |
|---|---|
| RingCentral_App_VMware_Plugin | ThinOS YYMM <version> RingCentral App VMWare Plugin package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |
| Common_printing | ThinOS YYMM <version> Common printing package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, Latitude 3440, Latitude 5440, and OptiPlex All-in-One 7410 |

ⓘ **NOTE:** After you upgrade to the latest version of ThinOS, you can only downgrade to ThinOS 9.1.3129 or later versions using Wyse Management Suite. If you want to downgrade to any previous version, you must use the USB Imaging Tool with Merlin images posted on the www.dell.com/support site.

ⓘ **NOTE:** For a given ThinOS release, you can install only the supported packages mentioned in the corresponding ThinOS Release Notes available at www.dell.com/support.

4. If you want to install the latest BIOS package, locate the package entry—ThinOS YYMM <version> BIOS package <version>—for your thin client model and click the download icon.

   For information about BIOS installation, see BIOS Installation.

# File naming convention

ThinOS application packages, ThinOS firmware, and BIOS packages support the following characters in their file names:

- Uppercase letter
- Lowercase letter
- Numeric character
- Special characters—period (.), hyphen-minus (-), and underscores (_)

If you use other characters in file names, the package installation fails. Other files that can be uploaded to the Wyse Management Suite server must follow the same naming convention.

7

# Upgrading ThinOS firmware

## Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite

### Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the new version of the firmware to upgrade.

### Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**. The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **OS Firmware Updates**.

   ⓘ **NOTE:** If you cannot locate the **OS Firmware Updates** option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse** and select the new version of the firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.
   The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

   ⓘ **NOTE:** There are chances that the upgrade might fail with event log stating **Failed to install**. In such an event, you may reboot the device and upgrade again.

   ⓘ **NOTE:** To optimize security, application performance, and stability, a design change has been made in ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

   ⓘ **NOTE:** There are chances that the ThinOS background might be in blue color and some features may not work. In this case, you have to reboot the device.

## 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 9.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 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 mentioned in the corresponding ThinOS Release Notes available at www.dell.com/support.

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. 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.

   **NOTE:** To optimize security, application performance, and stability, a design change has been made in ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

# Convert Ubuntu with DCA to ThinOS 2303, 2211, 2208, and 2205

### Prerequisites

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

**Table 9. Supported conversion scenarios**

| Platform | Ubuntu version | DCA-Enabler version |
|---|---|---|
| Latitude 3420 | 20.04 | 1.5.0-14 or later |
| OptiPlex 5400 All-in-One | 20.04 | 1.5.0-14 or later |
| Latitude 3440 | 22.04 | 1.7.0-20 or later |
| Latitude 5440 | 22.04 | 1.7.0-20 or later |
| OptiPlex All-in-One 7410 | 22.04 | 1.7.0-20 or later |

For details on how to install DCA-Enabler in Ubuntu operating system and upgrade it, see Install DCA-Enabler on Ubuntu

- **NOTE:** The device must have a factory-installed Ubuntu operating system. If you have custom installed the Ubuntu operating system, you cannot convert it to 2303, 2211, 2208, and 2205.

  **NOTE:** There are some languages that do not support the conversion from Ubuntu to ThinOS 2205. Dell Technologies recommends you to set Ubuntu to English language for the conversion process.
- Wyse Management Suite version 3.7 or later versions must be used to convert to 2303, 2211, 2208, and 2205.
- Ensure that you have connected the Ubuntu device to the external power source using the power adapter.
- Ensure you have enough ThinOS Activation devices licenses on Wyse Management Suite 3.7 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than the Ubuntu device number. If it is not larger, you cannot 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 Wyse Management Suite.

- Ensure you have downloaded the Ubuntu to ThinOS 2303, 2211, 2208, and 2205 conversion image.
- Extract the Ubuntu to ThinOS 2303, 2211, 2208, and 2205 conversion image to get the Conversion Installer file. **DTOS_Ubuntu_Installer_x.x-dtosx-amd64_signed.tar.gz** and ThinOS image **ThinOS_YYMM_9.x.pkg**.

  ⓘ **NOTE:** The ThinOS image **ThinOS_YYMM_9.x.pkg** can be used for downgrade in the future.

### Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the Conversion Installer file **DTOS_Ubuntu_Installer_x.x-dtosx-amd64_signed.tar.gz**
3. Go to **Apps & Data** > **OS Image Repository** > **ThinOS 9.x**, and click **Add Firmware file**.
4. Upload the ThinOS image **ThinOS_YYMM_9.x.pkg**.
5. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
6. Enter the policy name, select the group in which the Ubuntu device has been registered, and select **Generic Client** as OS type.
7. Click **Add app**, and select the conversion installer file that was uploaded before from the drop-down menu.
8. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
9. Select the platforms you want to convert in the **Platform Filter** drop-down menu.
10. Click **Save**.

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

11. In the next window, click **Yes** to schedule a job.
12. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.
13. 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 consumed automatically.

    ⓘ **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 has failed, 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 has failed, 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.

**Table 10. 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 Future packages | Failed to extract the ThinOS image, reschedule job |
| Error copying the DHC/ThinOS Future packages to recovery partition | Failed to copy the ThinOS image, reschedule job |
| ThinOS 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 |

# Install ThinOS from USB drive using Dell OS Recovery Tool

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

- OptiPlex 3000 Thin Client
- Latitude 3420
- OptiPlex 5400 All-in-One
- Latitude 3440
- Latitude 5440
- OptiPlex All-in-One 7410

For more information, see the Dell Wyse ThinOS Installation and ThinOS Activation License User Guide at www.dell.com/support

# Configuring a ThinOS 9.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 9.x-based thin client displays a message prompting you to restart the thin client immediately or postpone it to the next reboot for applying 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.

## Configuration comparison between ThinOS 8.6 and ThinOS 9.x

The following is an overview of the major device configuration changes between ThinOS 8.6 and ThinOS 9.x that simplifies the configuration process:

**Table 11. Configuration comparisons between ThinOS 8.6 and ThinOS 9.x**

| ThinOS 8.6 | ThinOS 9.x |
|---|---|
| ThinOS 8.6 requires INI files with complex parameter syntax to configure devices. | ThinOS 9.x configuration is completely menu driven. |
| ThinOS 8.6 user interface is a subset of all possible client configurations and is primarily designed for piloting devices. | ThinOS 9.x administrative user interface supports all client commands. |
| ThinOS 8.6 user interface menu configurations differed from Wyse Management Suite ThinOS menu–based profile configurations. | ThinOS 9.x shares a common administrative user interface with the Wyse Management Suite ThinOS 9.x profile. Hence all client configurations are identical when run from either interface. |

## ThinOS configuration grouping overview

During the deployment process, you must evaluate 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 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 12. ThinOS configuration grouping overview**

| Group Types | Configurations |
|---|---|
| Global device configurations | Privilege Settings including Admin Mode<br>Security Policy Settings<br>Remote Control Settings (VNC) |

Table 12. ThinOS configuration grouping overview (continued)

| Group Types | Configurations |
|---|---|
| | Management Settings<br>All other global configurations |
| Device configurations for a group of clients | Group-based Broker Configurations<br>Group-based Printer Settings<br>Group-based Time Zone Settings |
| Device configurations for a single device | Client-based Terminal Name<br>Client-based Location<br>Client-based Location and Custom 1, 2, 3 |
| Device configurations dynamically selected | ThinOS 8.6 Select Group with device configurations |
| Device configurations for an AD user group | ThinOS 8.6 SignOn=NTLM (AD.INI) with user configurations |
| User configurations for a single user | ThinOS 8.6 SignOn=Yes or NTLM with user configurations |

# ThinOS 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 system variables:

Table 13. ThinOS 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. |
| $DHCP (extra_dhcp_option) | Extra DHCP options for Windows CE unit, including 169, 140, 141, 166, 167.<br>For example, set a string test169 for option tag 169 in DHCP server, and set TerminalName=$DHCP(169) in wnos.ini. Check terminal name in GUI, and the terminal name will be test169. 166 and 167 is default for CCM MQTT Server and CCM CA validation in ThinOS. You must remap the options from GUI or INI 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 3 digits between separators. For example, 010.020.030.040.ini. Using it in conjunction with the left or right modifier helps to |

Table 13. ThinOS system variables (continued)

| Variable | Description |
|---|---|
| | define policy for 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 $xx is any of above parameters and the parameter i specifies the digits for the offset of right or left. |
| &Right($xx, i) or &Left($xx, i) | Specifies whether the variable is read from left or right. The $xx refers to any of the above System Variables. The option "i" specifies left or right offset digits. For example, the parameter TerminalName=CLT-$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:<br>● First four characters—CLT-<br>● 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. |

# Relationship between INI and Wyse Management Suite group based configurations

This section describes the relationship between INI file parameter–based configurations, and Wyse Management Suite group based configurations. Both INI files and Wyse Management Suite configuration processes have similar functionality. However, the implementation differs. Understanding this concept should greatly reduce the number of redundant configurations and help migrating devices from a file server with INI files to Wyse Management Suite.

Table 14. Relationship between INI and Wyse Management Suite group-based configurations

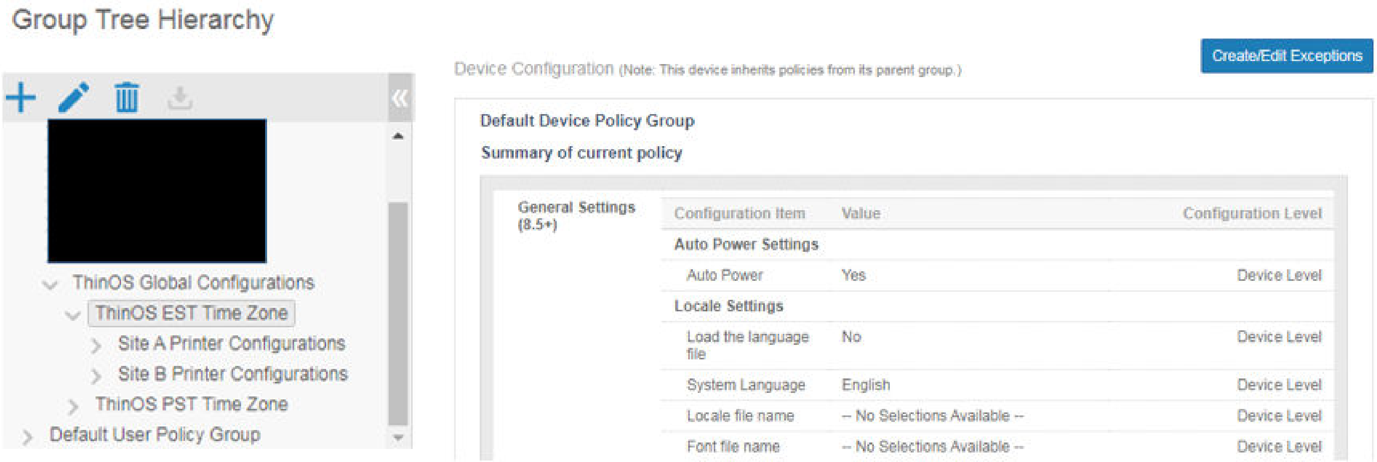
| Configuration | ThinOS 8.6 with INI | ThinOS 9.x with Wyse Management Suite |
|---|---|---|
| **Global configurations applied at boot to all clients**—When using Wyse Management Suite, client configuration policies that applies to all devices should be defined using a Wyse Management Suite Device Policy Parent Group. This is similar to wnos.ini configurations when using a file Server. | Global Configuration File (wnos.ini) | Groups and Config<br>Device Policy Parent Group |
| **Configurations applied at boot to a group of clients**—When using Wyse Management Suite, client configuration policies that apply to a group of device should be defined using Wyse Management Suite Device Policy Child Groups. This is similar to an INCLUDE file statement with part of a system variable that enables more than one client device to obtain the defined configurations. The advantage of Wyse Management Suite is that it enables multiple Child Group levels, hence allowing nesting of configurations. | Include parameter<br>(wnos\INC) | Groups and Config<br>Device Policy Child Groups |
| **Configurations applied at boot to a single client device**—When using Wyse Management Suite, client configuration policies that apply to a specific device can be completed using Wyse Management Suite Device Exceptions. This is similar to an INCLUDE file statement using a full system variable that allows only the selected client to obtain the defined configurations.<br>ⓘ **NOTE:** Device exceptions must be used when required and should be kept to a minimal number of configurations. | Include parameter<br>(WNOS\INC) | Devices<br>Device Exception |

**Table 14. Relationship between INI and Wyse Management Suite group-based configurations (continued)**

| Configuration | ThinOS 8.6 with INI | ThinOS 9.x with Wyse Management Suite |
|---|---|---|
| Excessive use of Device Exceptions or Device Exception configurations can affect performance and manageability. | | |
| **Device configurations dynamically selected from the ThinOS Login menu**—The Select Group feature in ThinOS enables you to dynamically select and load configurations and is often used to access multiple virtual environments. In Wyse Management Suite 2.0, this feature is supported only on ThinOS 9 devices.<br>The **Select Group** feature can be enabled under Wyse Management Suite **PRO Groups & Configs Device Policy Group** when creating a **Parent Group**. Select Group feature is not supported by Wyse Management Suite Device Policy Child Groups.<br>**NOTE:** The Select Group feature is not available when using Wyse Management Suite Standard. A Wyse Management Suite Pro license is required to enable this feature. | SelectGroup parameter<br>(WNOS\INI\GROUPS) | Groups and Configs<br>Device Policy Parent Group with Select Group Enabled |
| **User configurations applied at Login based on Active Directory Domain**—When using Wyse Management Suite, ThinOS configurations for a group of users can be defined by use of the Wyse Management Suite User Policy Group. This feature is similar to AD.INI functionality used by ThinOS 8.6 that dynamically applies configurations to ThinOS at SignOn (NTLM) based on the Active Directory Group Name.<br>**NOTE:** ThinOS 9.x Login type (under **Login Experience** > **Login Settings** and go to **Login Type**) must be set to Authenticate to domain controller at the Default Device Policy Group level for Active Directory Domain based configuration to function. If you are using the Active Directory group policy, the login type must be configured in the child group level of the device policies. | SignOn=NTLM,<br>(WNOS\INI\ AD.INI) | Groups and Configs<br>User Policy Group |
| **User configurations applied at Login based on Username**—When using Wyse Management Suite, ThinOS configurations for a single user is defined by use of Wyse Management Suite User Exceptions. It is similar to Username.INI functionality used by ThinOS 8.6 that dynamically applies configurations to ThinOS at Login (NTLM or Yes) based on username.<br>**NOTE:** User Exceptions should only be used when required and should be kept to a minimal number of configurations. Excessive use of User Exceptions or User Exception configurations can affect performance and manageability. | SignOn=Yes or NTLM<br>(WNOS\INI\username.ini) | Users<br>User Exceptions |

Wyse Management Suite can define device and user configurations for ThinOS and during boot ThinOS receives a device configuration payload from Wyse Management Suite. Additionally, a user configuration payload is received at Login.

For example, consider a scenario with device policies configured as shown in the following screenshot:



Group Tree Hierarchy

[redacted]

- ThinOS Global Configurations
  - ThinOS EST Time Zone
    - Site A Printer Configurations
    - Site B Printer Configurations
  - ThinOS PST Time Zone
- Default User Policy Group

Device Configuration (Note: This device inherits policies from its parent group.)

Create/Edit Exceptions

Default Device Policy Group

Summary of current policy

| General Settings (8.5+) | Configuration Item | Value | Configuration Level |
|---|---|---|---|
| | **Auto Power Settings** | | |
| | Auto Power | Yes | Device Level |
| | **Locale Settings** | | |
| | Load the language file | No | Device Level |
| | System Language | English | Device Level |
| | Locale file name | -- No Selections Available -- | Device Level |
| | Font file name | -- No Selections Available -- | Device Level |

**Figure 1. Device policy**

In this scenario, a client that is assigned to Site B Printer Configurations receives a device payload based on the following:

- ThinOS global configurations
- ThinOS EST time zone configurations
- Site B printer configurations
- Device exception configurations

Similarly, at Login, Wyse Management Suite applies user policies based on the Active Directory Group Name or User Exception Policies based on username information.

For more information on how to configure active directory group settings and user exceptions, see the Wyse Management Suite Administrators Guide at www.dell.com/support.

# 9

# BIOS Installation

## Upgrade BIOS

### Prerequisites

- Download the BIOS file from www.dell.com/support to your device.
- If you are upgrading BIOS using Wyse Management Suite, register the thin client to Wyse Management Suite.

### About this task

ⓘ **NOTE:** On thin clients that run ThinOS versions earlier than ThinOS 9.1.6108, you must upgrade the OS image first, and then upgrade the BIOS after the OS image is successfully upgraded. Do not upgrade the BIOS and the OS image together. If you upgrade the BIOS and the OS image together, the BIOS upgrade is ignored, and you cannot upgrade the BIOS to the ignored version anymore. You must upgrade the BIOS to another version.

### Steps

1. Open the Admin Policy Tool on the thin client or go to the ThinOS 9.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 list, 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 www.dell.com/support.

   ⓘ **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.

## 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 v2.1 Administrator's Guide* at www.dell.com/support.

  ⓘ **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 WMS server, the **Current BIOS Admin password** option in 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 9.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 if you are setting a new password, and then the 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 new BIOS password and then reboot the thin client, the new BIOS password is synced to 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.

10

# Downgrade to previous versions of ThinOS

You can only downgrade to ThinOS 9.1.3129 or later versions using Wyse Management Suite. If you want to downgrade to any version prior to ThinOS 9.1.3129, you must use Merlin images posted on the www.dell.com/support site.

ⓘ **NOTE:** If you want to downgrade to ThinOS 9.0, you must clear TPM or PTT in the BIOS and then use the USB imaging tool and Merlin images to downgrade.

ⓘ **NOTE:** You cannot downgrade to ThinOS 8.6_606 or previous versions, if you are running the systems with SSD devices.

ⓘ **NOTE:** You must install the application packages after you downgrade to ThinOS 8.6 using Merlin Image.

11

# Delete ThinOS 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 client.
2. From the system menu, go to **System Tools** > **Packages**.
   All the installed ThinOS 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**.

# 12

# Resources and support

## Accessing documents using the product search

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, `OptiPlex 3000 Thin Client` . A list of matching products is displayed.
3. Select your product.
4. Click **Documentation**.

## Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to www.dell.com/support.
2. Click **Browse all products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **OptiPlex Thin Client**.
6. Click **OptiPlex 3000 Thin Client**.
7. Click **Select this Product**.
8. Click **Documentation**.

# 13

# Contacting Dell

### Prerequisites

ⓘ **NOTE:** If you do not have an active internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

### About this task

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

### Steps

1. Go to www.dell.com/support.
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.