Dell ThinOS 9.x 2402, 2405, 2408, and 2411

Migration Guide

Notes, cautions, and warnings

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

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

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

Contents

Introduction

This guide provides instructions to migrate from Ubuntu and ThinOS 9.1.3129 or later versions to ThinOS 2411 using Wyse Management Suite 4.0 or later versions.

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 firmware from the Support | Dell 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.

When converting a device from different operating system to ThinOS 2303 or later, or when installing the ThinOS 2303 or later recovery image, ThinOS sets the following BIOS settings during the initial boot:

- BIOS password: **Fireport**
- SATA/NVMe Operation: **AHCI/NVMe**
- Integrated network adapter: Set to **Enabled** (set to disable PXE boot support)
- Wake-on-LAN: **LAN only**

  (i) **NOTE:** For OptiPlex 3000 Thin Client with SFP module, the option is set to **LAN or SFP NIC**.

- Enable Secure Boot: **ON**
- Enable USB Boot Support: **OFF**
- Enable USB Wake Support: **ON**
- Deep Sleep Control: **Disabled**

(i) **NOTE:** These BIOS settings changes only apply to devices with the BIOS password set to **Fireport** or with an empty password field.

(i) **NOTE:** Third-party packages that are released before 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
- Latitude 5450
- OptiPlex All-in-One 7410
- OptiPlex All-in-One 7420

Supported Wyse Management Suite versions

The following are the supported Wyse Management Suite versions:

- Wyse Management Suite 4.0, 4.1, 4.2, 4.3, and 4.4

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 Wyse Management Suite page. For information about Wyse Management Suite manuals, go to the Wyse Management Suite product page at Support | Dell.

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 Support | Dell.
- Direct upgrades from ThinOS 8.6 to ThinOS 2205 or later versions are not possible 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 the BIOS.

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.
- Starting with ThinOS 2402 onward, 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.
- Starting with ThinOS 2402, 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 will not download or install 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, clicking **Next Reboot**:
  - Displays the notification 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.
- If the event log fails to install, the upgrade may fail. 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 Support | Dell for more information.

ⓘ **NOTE:** After upgrading to ThinOS 2402 or later versions, all application packages that are released before 2205, Microsoft AVD package that is released before 2311, and the Zoom AVD, Zoom Citrix, and Zoom Horizon packages are removed automatically and cannot be installed again. You must install the latest application packages.

Wyse Management Suite Environment Automation with DHCP and DNS

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 you 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 1. 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) ⓘ **NOTE:** Supported from ThinOS 9.1.6108. Do not set this value if your current version is earlier than 9.1.6108.	Option 20100 (String)	_WMS_MGMTV2 (Text) ⓘ **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)	NA	_ 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	Option 202 (String)	Option 20200 (String)	_WMS_GROUPTOKENV2 (Text)

Table 1. DHCP and DNS configuration for Wyse Management Suite (continued)

Environment	Definition	IPv4 DHCP User-Defined Option	IPv6 DHCP User-Defined Option	DNS Resource Record
	Wyse Management Suite to associate the ThinOS client to the device group Policy.	(i) **NOTE:** Supported from ThinOS 9.1.6108. Do not set this value if your current version is earlier than 9.1.6108.		(i) **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.

(i) **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 with IPv4 DHCP option tags

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

Table 2. Registering device with IPv4 DHCP option tags

Option Tag	Description
• Name—WMS • Data Type—String • Code—201 • Description—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com`, where wmsserver.acme.com is the fully qualified domain name of the server hosting the Wyse Management Suite. (i) **NOTE:** HTTPS:// is not required in the Wyse Management Suite URL.
• Name—WMS • Data Type—String • Code—201 • Description—Secure WMS Server	This tag points to the secure Wyse Management Suite server.
• Name—MQTT • Data Type—String • Code—166 • 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. (i) **NOTE:** MQTT is optional for Wyse Management Suite 2.0 and later versions.
• Name—CA Validation • Data Type—String • Code—167 • Description—Certificate Authority Validation	• You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud. • Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. • 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. (i) **NOTE:** CA Validation is optional for Wyse Management Suite 2.0 and later versions. However, it is recommended to configure this option tag.
• Name—Group Registration Key • Data Type—String • Code—199 • Description—Group Registration Key	The tag directs the device to retrieve the Group Registration Key for Wyse Management Suite. For example, in SCDA-DTos91SalesGroup, 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 \(backslash), "(double quotes), '(single quote) are not allowed. The Group Registration Key is case-sensitive.

Table 2. Registering device with IPv4 DHCP option tags (continued)

Option Tag	Description
	ⓘ **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 an unmanaged group. Therefore, It is recommended to configure the Group Token key.
● Name—Group Registration Key ● Data Type—String ● Code—202 ● Description—Secure Group Registration Key	The tag directs the device to retrieve 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.

WMS auto discovery by IPv6 DHCP option

ThinOS 2411 supports WMS auto discovery by IPv6 DHCP option. The IPv6 DHCP option tags for WMS auto discovery are listed below:

Table 3. WMS auto discovery by IPv6 DHCP option

Option Tag	Description
● Name—WMS ● Data Type—String ● Code—16500 ● Description—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com`, where wmsserver.acme.com is the fully qualified domain name of the server hosting the Wyse Management Suite. ⓘ **NOTE:** HTTPS:// is not required in the Wyse Management Suite URL.
● Name—WMS ● Data Type—String ● Code—20100 ● Description—Secure WMS Server	This tag points to the secure Wyse Management Suite server.
● Name—CA Validation ● Data Type—String ● Code—16700 ● Description—Certificate Authority Validation	● You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud. ● Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. ● 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. ⓘ **NOTE:** CA Validation is optional for Wyse Management Suite 2.0 and later versions. However, it is recommended to configure this option tag.

Table 3. WMS auto discovery by IPv6 DHCP option (continued)

Option Tag	Description
• Name—Group Registration Key • Data Type—String • Code—19900 • Description—Group Registration Key	The tag directs the device to retrieve the Group Registration Key for Wyse Management Suite. For example, in SCDA-DTos91SalesGroup, 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 \ (backslash), "(double quotes), '(single quote) are not allowed. The Group Registration Key is case-sensitive. (i) **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 an unmanaged group. Therefore, It is recommended to configure the Group Token key.
• Name—Group Registration Key • Data Type—String • Code—20200 • Description—Secure Group Registration Key	The tag directs the device to retrieve the secure Group Registration Key for Wyse Management Suite.

(i) **NOTE:** If only IPv6 is present in your network and IPv4 is absent, it takes about 5 minutes for the IPv4 DHCP to time out. After this, the system automatically discovers WMS from IPv6 DHCP. Ensure that IPv4 is disabled in your WMS policy; otherwise, each reboot results in a 5-minute wait for the IPv4 DHCP to time out.

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 4. Configure devices with 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. (i) **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. (i) **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. (i) **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.

Table 4. Configure devices with DNS SRV record (continued)

Option tag	Description
WMS CA Validation (_WMS_CAVALIDATION, Type Text)	● 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. ● 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. ● 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. ⓘ **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**.

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 directly from the ThinOS GUI. This configuration must be done individually on each thin client.

Steps

1. From the desktop menu of the thin client, go to **System Setup** > **Central Configuration**.
   The **Central Configuration** window is displayed.
   (i) **NOTE:** Privilege must be set to **High** or Admin Mode must be activated to access to the ThinOS Central Configuration menu.

2. Select the **Enable WMS Advanced Settings** 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 that you have provided. Ensure that the network is not blocking the default ports, which are 443 and 1883.

   (i) **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 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 2.0 Administrator's guide* at Support | Dell.

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 from Support | Dell.
- 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** to obtain the following 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.

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

Upgrade DCA-Enabler through Wyse Management Suite on Ubuntu

Prerequisites

- Download DCA-Enabler from Support | Dell.
- 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 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 installs on Ubuntu devices. You can check the job status from the Wyse Management Suite server Jobs page.

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.
- 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**

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

- Ensure that DCA-Enabler 1.5.0-14 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 section.

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

Download ThinOS firmware, BIOS, and application packages

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

Steps

1. Go to the Support | Dell site.
2. Locate the required ThinOS Image entry and click the download icon.

Table 5. ThinOS 2411 image

Scenario	ThinOS image title
Upgrade your ThinOS 9.1.3129 or later versions to 2411 9.5.4070	ThinOS 9.1.3129 or later to ThinOS 2411 9.5.4070 Image file for Dell Wyse 5070, 5470 and 5470 All-in-One Thin Clients, Dell OptiPlex 3000 Thin Client, Dell Latitude 3420, 3440, 5440 and 5450, Dell OptiPlex 5400 All-in-One, Dell OptiPlex All-in-One 7410, and Dell OptiPlex All-in-One 7420
Ubuntu to ThinOS 2411 conversion image	ThinOS 2411 Ubuntu conversion image for Dell Latitude 3420, 3440, 5440, and 5450, Dell OptiPlex 5400 All-in-One, Dell OptiPlex All-in-One 7410, and Dell OptiPlex All-in-One 7420

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

Table 6. ThinOS packages

ThinOS packages	ThinOS image title
Citrix_Workspace_App	ThinOS YYMM <version> Citrix package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
VMware_Horizon	ThinOS YYMM <version> VMware Horizon package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
VMware_Horizon_Client SDK (The package cannot be installed with VMware_Horizon simultaneously)	ThinOS YYMM <version> VMware Horizon package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Teradici_PCoIP	ThinOS YYMM <version> Teradici PCoIP package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Microsoft_AVD	ThinOS YYMM <version> Microsoft AVD package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Imprivata_PIE	ThinOS YYMM <version> Imprivata package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client,

Table 6. ThinOS packages (continued)

ThinOS packages	ThinOS image title
	OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Zoom_Universal	ThinOS YYMM <version> Zoom Universal package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Jabra	ThinOS YYMM <version> Jabra headsets package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
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, Latitude 5450, OptiPlex All-in-One 7410, and OptiPlex All-in-One 7420
Cisco_WebEx_VDI	ThinOS YYMM <version> Cisco Webex VDI package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Cisco_WebEx_Meetings_VDI	ThinOS YYMM <version> Cisco Webex Meetings package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Cisco_Jabber	ThinOS YYMM <version> Cisco Jabber package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
HID_Fingerprint_Reader	ThinOS YYMM <version> HID Fingerprint Reader package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Identity_Automation_QwickAccess	ThinOS YYMM <version> Identity Automation QwickAccess package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
ControlUp_VDI_Agent	ThinOS YYMM <version> ControlUp VDI Agent package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
RingCentral_App_VMware_Plugin	ThinOS YYMM <version> RingCentral App VMware Plugin package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Common_Printing	ThinOS YYMM <version> Common printing package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Liquidware_Stratusphere_UX_Connector_ID_Agent	ThinOS YYMM <version> Liquidware package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Amazon_WorkSpaces_Client	ThinOS YYMM <version> Amazon WorkSpaces Client package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex

Table 6. ThinOS packages (continued)

ThinOS packages	ThinOS image title
	3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
Lakeside_Virtual_Agent	ThinOS YYMM <version> Lakeside Virtual Agent package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
ThinOS_Telemetry_Dashboard	ThinOS YYMM <version> ThinOS Telemetry Dashboard package <version> for Wyse 3040 and 5070 Thin Clients, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
UXM_Endpoint_Agent	ThinOS YYMM <version> UXM Endpoint Agent package <version> for Wyse 5070 Thin Client, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420
eG_VM_Agent	ThinOS YYMM <version> eG VM Agent package <version> for Wyse 5070 Thin Client, Wyse 5470 Mobile Thin Client, Wyse 5470 All-in-One Thin Client, OptiPlex 3000 Thin Client, OptiPlex 5400 All-in-One, Latitude 3420, 3440, 5440, 5450, OptiPlex All-in-One 7410 and 7420

ⓘ **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 Support | Dell site.

ⓘ **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.

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.

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**.

   (i) **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.

   (i) **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.

   (i) **NOTE:** To enhance security, application performance, and stability, a design change has been implemented in ThinOS 2205. This change affects the installation of third-party applications, such as Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path compared to 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. After upgrading to ThinOS 2205 or later versions, install the latest version of any required third-party applications.

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**.

(i) **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.

   (i) **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**.

   (i) **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.

   (i) **NOTE:** To enhance security, application performance, and stability, a design change has been implemented in ThinOS 2205. This change affects the installation of third-party applications, such as Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path compared to 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. After upgrading to ThinOS 2205 or later versions, install the latest version of any required third-party applications.

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
● Latitude 5450
● OptiPlex All-in-One 7410
● OptiPlex All-in-One 7420

For more information, see the Dell ThinOS Installation and ThinOS Activation License User Guide at Support | Dell.

Converting to ThinOS

Convert Ubuntu with DCA to ThinOS

Prerequisites

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

Table 7. Supported conversion scenarios

Platform	Ubuntu version	DCA-Enabler version
Latitude 3420	20.04	1.7.1-61 or later
OptiPlex 5400 All-in-One	20.04	1.7.1-61 or later
Latitude 3440	22.04	1.7.1-61 or later
Latitude 5440	22.04	1.7.1-61 or later
Latitude 5450	22.04	1.7.1-61 or later
OptiPlex All-in-One 7410	22.04	1.7.1-61 or later
OptiPlex All-in-One 7420	22.04	1.7.1-61 or later

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

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

- Wyse Management Suite version 4.0 or later must be used to convert to ThinOS.
- Ensure that you have connected the Ubuntu device to the external power source using the power adapter.
- Ensure that you have enough ThinOS Activation device licenses on Wyse Management Suite.
- 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 WMS manually.
- Ensure that you have downloaded the Ubuntu to ThinOS conversion image.
- Extract the Ubuntu to ThinOS 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**.

(i) **NOTE:** The ThinOS image **ThinOS_YYMM_9.x.pkg** can be used for future downgrades if needed.

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**.
    > (i) **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.
    > (i) **NOTE:** After you register the converted ThinOS device to Wyse Management Suite, the ThinOS activation devices license is consumed automatically.

    > (i) **NOTE:** After conversion, ThinOS is in the factory default status. ThinOS must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

    > (i) **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.

Table 8. 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

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 9. 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 10. ThinOS configuration grouping overview

Group Types	Configurations
Global device configurations	- Privilege Settings including Admin Mode - Security Policy Settings - Remote Control Settings (VNC) - Management Settings

Table 10. ThinOS configuration grouping overview (continued)

Group Types	Configurations
	● All other global configurations
Device configurations for a group of clients	● Group-based Broker Configurations ● Group-based Printer Settings ● Group-based Time Zone Settings
Device configurations for a single device	● Client-based Terminal Name ● Client-based Location ● 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 11. 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.
$DHCP (extra_dhcp_option)	Extra DHCP options for ThinOS unit, including 169, 140, 141, 166, 167. For example, set a string **test169** for the **tag169** option in the DHCP server, and set **TerminalName=$DHCP(169)** in the Wyse Management Suite policy. Check the terminal name in the UI, and the terminal name is **test169**. **166** and **167** is default for the Wyse Management Suite MQTT Server and Wyse Management Suite CA validation in ThinOS. You must remap the options from the UI or the Wyse Management Suite policy if you want to use **$DHCP(166)** or **$DHCP(167)**.
$DN	Sign on domain name
$TN	Terminal name
$UN	Sign on username
$SUBNET	For subnet notation, the format is **{network_address}_{network_mask_bits}**. For example, if the IP address is 10.151.120.15, the network mask is 255.255.255.0, and 10.151.120.0_24 is used.
$FIP	IP address is used in fixed format with three digits between separators. For example, 010.020.030.040.ini. Using it with the left or right modifier helps to define policy for the subnet. For example, include=&Left($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

Table 11. ThinOS system variables (continued)

Variable	Description
Right($xx, i) or and Left($xx, i)	Specifies that the variable is to be read from left or right. The **$xx** is any of above parameters, and the parameter **i** specifies the digits for the offset of right or left.
&Right($xx, i) or &Left($xx, i)	Specifies whether the variable is read from left or right. The **$xx** is any of the above System Variables. The option **i** specifies left or right offset digits. For example, in the parameter **TerminalName=CLT-SNRIGHT$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: ● First four characters—CLT- ● The rest—The last right-most seven digits of the thin client serial number. The resulting terminal name is displayed as CLT-MA00256.
$AT	**Asset Tag** must be enabled in the BIOS settings. **$AT** can be used as terminal name, and the length is limited to 32 characters.

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 can reduce the number of redundant configurations and help migrate devices from a file server with INI files to Wyse Management Suite.

Table 12. Relationship between INI and Wyse Management Suite group-based configurations

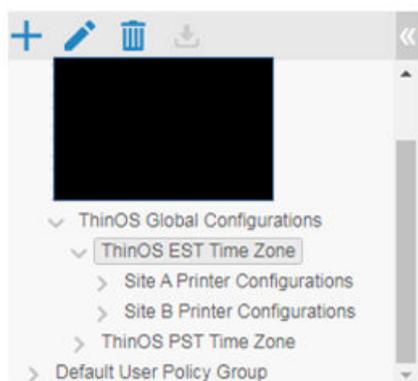| Configuration	ThinOS 8.6 with INI	ThinOS 9.x with Wyse Management Suite
Global configurations applied at boot to all clients—When using Wyse Management Suite, client configuration policies apply to all devices should be defined using a Wyse Management Suite Device Policy Parent Group. This is similar to wnos.ini configurations when using a file Server.	Global Configuration File (wnos.ini)	● Groups and Config ● 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 ● (wnos\INC) I	● Groups and Config ● 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. (i) **NOTE:** Device exceptions must be used when required and should be kept to a minimal number of configurations. Excessive use of Device Exceptions or Device Exception configurations can affect performance and manageability.	● Include parameter ● (WNOS\INC) I	● Devices ● Device Exception
● **Device configurations dynamically selected from the ThinOS Login menu**—The Select Group feature in ThinOS enables you to dynamically select and load configurations	● SelectGroup parameter ● (WNOS\INI\GROUPS)	● Groups and Configs ● Device Policy Parent Group with Select Group Enabled

Configuration	ThinOS 8.6 with INI	ThinOS 9.x with Wyse Management Suite
and is often used to access multiple virtual environments. In Wyse Management Suite 2.0, this feature is supported only on ThinOS 9 devices. ● The **Select Group** feature can be enabled under Wyse Management Suite **PRO Groups & Configs Device Policy Group** when creating a **Parent Group**. The select Group feature is not supported by Wyse Management Suite Device Policy Child Groups. ⓘ **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.		
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. ⓘ **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 ● (WNOS\INI\ AD.INI)	Groups and Configs 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. ⓘ **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 ● (WNOS\INI\username.ini)	● Users ● 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. Also, 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

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 about how to configure active directory group settings and user exceptions, see the Wyse Management Suite Administrators Guide at Support | Dell.

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:** On thin clients that run ThinOS versions earlier than ThinOS 9.1.6108, 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 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 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.

   ● From ThinOS 2402, if a monitor is not connected to Wyse 5070, the BIOS update fails. After the monitor is connected, the BIOS update is triggered immediately.
   ● If a power adapter is not connected on the Wyse 5470, 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 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**.

   (i) **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.

   (i) **NOTE:** If you change the BIOS password using a select group, it requires a reboot to take effect.

   (i) **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.

   (i) **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.

   (i) **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.

Downgrade to previous versions of ThinOS

You can only downgrade to ThinOS 9.1.3129 or later versions using Wyse Management Suite. To downgrade to any version prior to 9.1.3129, you must use the Merlin images available on the Dell Support site.

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

ⓘ **NOTE:** Downgrading to ThinOS 8.6_606 or earlier versions is not possible if your system is equipped with SSD devices.

ⓘ **NOTE:** After downgrading to ThinOS 8.6 using a Merlin image, you must reinstall the application packages.

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**.

   (i) **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**.

13

Resources and support

Accessing documents using the product search

1. Go to Support | Dell.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, `OptiPlex 7410 All-In-One` or `Latitude 3440 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 Support | Dell.
2. Click **Browse all products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **Wyse Software**.
6. Click **Wyse ThinOS** .
7. Click **Select this Product**.
8. Click **Documentation**.

Contacting Dell

Prerequisites

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.

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, follow the steps.

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.