Dell Wyse ThinOS

Version 9.1 Migration Guide

April 2021
Rev. A01

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

1

Introduction

This guide contains instructions to migrate from ThinOS 8.6 to ThinOS 9.1 using Wyse Management Suite 3.1.

NOTE: All device settings are erased after you upgrade from ThinOS 8.6 to 9.1 except the Wyse Management Suite server settings, wireless connections, wireless certificates, and proxy settings. You must back up your device settings before you start the upgrade process.

The overall migration process includes the following tasks:

1. Register the thin client to the Wyse Management Suite server using any of the following methods:
   - Automate the Wyse Management Suite server and Group Registration Token discovery using the DHCP or DNS records —see Register ThinOS devices by using DHCP option tags and Configuring devices by using DNS SRV record.
   - Manually configure the Wyse Management Suite server and Group Registration Token information using the ThinOS 8.6 user interface—see Register ThinOS devices using Wyse Device Agent.
2. Optionally, add a ThinOS 8.6-based device to a policy group in Wyse Management Suite to retain the INI file configurations —see Relationship between INI file based and Wyse Management Suite group based configuration.
3. Download the ThinOS 9.1 firmware from the www.dell.com/support site—see Download the ThinOS firmware.
4. Upgrade the ThinOS 8.6 firmware to ThinOS 9.1—see Upgrade ThinOS 8.6 to ThinOS 9.1.
   NOTE: Make sure that the 5070 BIOS version is 1.3.1 or later before upgrading to ThinOS 9.1. If you upgrade to ThinOS 9.1 with earlier BIOS version and then upgrade the BIOS version to 1.3.1 or later, it may fail to boot up the devices.
5. Configure the ThinOS 9.1-based device using Wyse Management Suite version 3.1—see Configuring a new ThinOS 9.1 client using Wyse Management Suite 3.1.

NOTE: Once the system is upgraded to ThinOS 9.1, if the BIOS password is set as default or if the password field is empty, then the **Secure Boot** is enabled automatically. If the BIOS password is not set as default, you must enable **Secure Boot** through Wyse Management Suite or admin policy tool.

NOTE: You cannot boot into ThinOS 9.1 when you perform the following operations:

- Disable the on-board Network Interface Card (NIC), Trusted Platform Module (TPM), or Platform Trust Technology (PTT).
- Clear TPM or PTT.
- Reset BIOS to factory default settings.

English-language user—Do not modify any language settings in Wyse Management Suite. The default language is English after you upgrade from ThinOS 8.6.

Multilanguage user—ThinOS 9.1 supports nine languages—English, German, French, Italian, Spanish, Japanese, Chinese Traditional, Chinese Simplified, and Korean. Users of all regions must use the English language firmware image. There is no separate firmware image for Japanese language. The firmware image includes the font and language packages for all the nine languages. You do not need a separate font and language package. You must set the region language in Wyse Management Suite before upgrade from ThinOS 8.6. After the device upgrade process is complete and checked in to the Wyse Management Suite server, the user interface language is changed to the language that you have configured in Wyse Management Suite. You can change the language from either Wyse Management Suite or ThinOS interface.

NOTE: When you upgrade from ThinOS 9.0 to 9.1, the thin client downloads all the application packages that are applicable to 9.1. After you upgrade to 9.1, all the application packages are removed and you must reinstall the application packages. Dell Technologies recommends you to upgrade from ThinOS 9.0 to 9.1 without installing the application packages. If you add multiple application packages along with the operating system image in the same Wyse Management Suite group, the upgrade may fail due to the low disk space. In this scenario, you must reset to factory default settings for upgrading the ThinOS client again.

NOTE: If you are using ThinOS 9.0.1136, you will not be able to upgrade the operating system firmware or install application packages post September 2021. You can update the operating system firmware or install the application packages by disabling the time server on ThinOS and changing the system time to August 2021. Dell Technologies recommends you to update to ThinOS 9.1.1131 or later version where this issue is resolved.

Downgrade to ThinOS 8.6 or 9.0—If you want to downgrade to ThinOS 8.6 or 9.0, disable the secure boot option in the BIOS setup. Downgrading ThinOS 9.1 to ThinOS 8.6 or 9.0 through Wyse Management Suite is not supported. You can downgrade to ThinOS 8.6 or 9.0 by using the USB Imaging Tool and 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 if you are running the systems with SSD devices.

NOTE: You must install the application packages after you downgrade from ThinOS 9.1 to ThinOS 8.6 through merlin image.

Supported systems

The following systems are supported on ThinOS 9.1:

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client

Supported Wyse Management Suite versions

The following are the supported Wyse Management Suite versions:

- Wyse Management Suite 3.1 Standard or later versions
- Wyse Management Suite 3.1 Pro (on-premises) or later versions
- Wyse Management Suite 3.1 Pro (cloud) or later versions

Wyse Management Suite default communications are handled over port 443 and MQTT communications over port 1883. WMS and MQTT 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.

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 after you reset your device to factory default settings.

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 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.	Option 199 (String)	_ WMS_GROUPTOKEN (Text)

It is recommended that you do not define more than one type of management or configuration delivery method. Ensure that all Wyse Device Manager (WDM) and file server configurations that are provided by DHCP or DNS are disabled when defining ThinOS Wyse Management Suite automation values.

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:

NOTE: It is recommended that you configure all the DHCP options including the optional MQTT, Group Token, and CA Validation tags.

Table 2. Registering device by using DHCP option tags

Option Tag	Description
Name—WMS Data Type—String Code—165	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. **NOTE:** HTTPS:// is not required in the Wyse Management Suite URL.

Table 2. Registering device by using DHCP option tags (continued)

Option Tag	Description
Description—WMS Server FQDN	
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. **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 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 com@Wedding2020munication between the client and the Wyse Management Suite server. **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 Data Type—String Code—199 Description—Group Registration Key	This tag directs to the Group Registration Key for the Wyse Management Suite agent. **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.

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)	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. **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.
(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. **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. **NOTE:** Group Token is optional for Wyse Management Suite 2.0 and later versions on private cloud.

Table 3. Configuring devices by using DNS SRV record

Option tag	Description
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. 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.

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. Go to **WDA** > **WMS**, and enter the **Group Registration Key** as configured by your administrator for the wanted group.
3. Select the **Enable WMS Advanced Settings** check box.
4. 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.
5. 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.

   NOTE: If you publish **WDA settings** or **WMS settings** policies on the Wyse Management Suite server, ensure that you specify the Group prefix, Group token field, and enable the Show Advanced Configuration option for providing the Wyse Management Suite server details. If not specified, the Wyse Management Suite Group Registration Key is cleared and the Wyse Management Suite server is changed to the default URL—https://us1.wysemanagementsuite.com on the client side.

6. 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.
7. 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.
8. Click **OK**.
   The device checks in to the Wyse Management Suite and the policy settings are applied.

4

Add a ThinOS 8.6 device to a group in Wyse Management Suite

This section is recommended for ThinOS 8.6 users transitioning from file server configuration and imaging to Wyse Management Suite. ThinOS 9.1 does not support FTP and WDM. The file storage and device management features are replaced by Wyse Management Suite.

About this task

Adding a ThinOS 8.6 device to a group in Wyse Management Suite allows you to maintain your current INI file based configuration and file server imaging while placing their ThinOS 8.6 clients under Wyse Management Suite. The process can be accomplished as follows:

Steps

1. On the Wyse Management Suite console, go to **Groups & Configs**, create a device policy group for each file server or Wyse Device Management dynamic device policy (DDC) group. Ensure that you define a unique group token value for group.
2. For each Wyse Management Suite device policy group, select **Edit Policies** and select **ThinOS** to define policies for the ThinOS 8.6 client group. If prompted for the Wyse Management Suite configuration mode, select **Advanced Configuration**.
3. From the Wyse Management Suite **Advanced Device Configuration** option, select **Central Configuration** and define the file server or path, user account, and password values for your current ThinOS 8.6 file server. Click **Save & Publish** and repeat the same step for each file server or Wyse Device Management DDC group. Ensure that the protocol is defined as part of your file server or path entry, or ThinOS 8.6 assumes the protocol as FTP.
4. Replace all environmentally or locally defined client file server and Wyse Device Management information with Wyse Management Suite, MQTT Server and Group Token information. For information about how to configure Wyse Management Suite using DHCP Options, DNS Records, or manually from the ThinOS client configuration menu, see the following sections:
   - Wyse Management Suite Environment Automation (DHCP or DNS)—see Register ThinOS devices by using DHCP option tags and Configuring devices by using DNS SRV record.
   - Wyse Management Suite Manual Configuration (ThinOS UI)—see Register ThinOS devices using Wyse Device Agent.
5. Restart the thin client.

   The thin client performs the following tasks automatically after reboot:
   - Discovers a Wyse Management Suite server and completes check-in based on the Group Token information. This process includes receiving file server configuration information from the Wyse Management Suite group that is assigned to the ThinOS 8.6 client.
   - Checks the file server, retrieve, and apply configuration data from the wnos.ini (and supporting files), and completes any required image updates from the images on the file server.

5

Download the ThinOS firmware, BIOS, and application packages

About this task

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 9.1.2101 image

Scenario	ThinOS image title
Upgrade your ThinOS 9.1.1131 to 9.1.2101	**ThinOS 9.1.1131 to ThinOS 9.1.2101 Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Upgrade your ThinOS 9.0.x to 9.1.2101	**ThinOS 9.0 to ThinOS 9.1.2101 Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Install the ThinOS 9.1.2101 Merlin image using USB Imaging Tool	**ThinOS 9.1.2101 Merlin Image file for Dell Wyse 5070 Thin Clients**.
	ThinOS 9.1.2101 Merlin Image file for Dell Wyse 5470 Thin Clients.
	ThinOS 9.1.2101 Merlin Image file for Dell Wyse 5470 All-in-One Thin Clients.
	ThinOS 9.1.2101 Merlin Image file for Dell Wyse 3040 Thin Clients.

Table 5. ThinOS 9.1.1131 image

Scenario	ThinOS image title
Upgrade your ThinOS 8.6 to 9.1.1131	**ThinOS 8.6 to ThinOS 9.1.1131 Base Image file for Dell Wyse 5070, 5470 and 5470 All-in-One Thin Clients**.
	ThinOS 8.6 to ThinOS 9.1.1131 Base Image file for Dell Wyse 5070, 5470 and 5470 All-in-One Thin Clients with PCoIP.
	ThinOS 8.6 to ThinOS 9.1.1131 Base Image file for Dell Wyse 3040 Thin Clients.
	ThinOS 8.6 to ThinOS 9.1.1131 Base Image file for Dell Wyse 3040 Thin Clients with PCoIP.
Upgrade your ThinOS 9.0 to 9.1.1131	**ThinOS 9 to ThinOS 9.1.1131 Base Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Install the ThinOS 9.1.1131 Merlin image using USB Imaging Tool	**ThinOS 9.1.1131 Merlin Image file for Dell Wyse 5070 Thin Clients**.
	ThinOS 9.1.1131 Merlin Image file for Dell Wyse 5470 Thin Clients.
	ThinOS 9.1.1131 Merlin Image file for Dell Wyse 5470 All-in-One Thin Clients.
	ThinOS 9.1.1131 Merlin Image file for Dell Wyse 3040 Thin Clients.

NOTE: If you are using the Dell Wyse USB Imaging Tool to install the ThinOS image on a single client, you must download the ThinOS 9.1 Merlin image

The image package is downloaded to your system.

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

Table 6. ThinOS packages

ThinOS packages	ThinOS image title
Citrix Workspace app	**ThinOS 9.1 <version> Citrix package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
VMware Horizon	**ThinOS 9.1 <version> VMware Horizon package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Teradici PCoIP	**ThinOS 9.1 <version> Teradici PCoIP package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Microsoft WVD	**ThinOS 9.1 <version> Microsoft WVD package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Imprivata PIE	**ThinOS 9.1 <version> Imprivata package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Zoom Horizon	**ThinOS 9.1 <version> Zoom Horizon package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Zoom Citrix	**ThinOS 9.1 <version> Zoom Citrix package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Jabra	**ThinOS 9.1 <version> Jabra headsets package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
EPOS Connect	**ThinOS 9.1 <version> EPOS Connect package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Cisco WebEx VDI	**ThinOS 9.1 <version> Cisco Webex VDI package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Cisco WebEx Meetings	**ThinOS 9.1 <version> Cisco Webex Meetings package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Cisco Jabber	**ThinOS 9.1 <version> Cisco Jabber package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
HID Fingerprint Reader	**ThinOS 9.1 <version> HID Fingerprint Reader package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.

4. Extract the downloaded package. The image filename depends on your hardware model. For example, A10Q_wnos or X10_wnos.

   NOTE: After you upgrade to ThinOS 9.1, you can only downgrade to ThinOS 8.6 by using the USB Imaging Tool with Merlin Images posted on the www.dell.com/support site. Once the system is upgraded to ThinOS 9.1, if the BIOS password is set as default or if the password field is empty, then the **Secure Boot** is enabled automatically. If you want to downgrade to ThinOS 8.6, disable the secure boot option in the BIOS. If you want to downgrade to ThinOS 9.0, you must clear TPM or PTT in the BIOS.

   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.

5. If you want to install the latest BIOS package, locate the package entry—ThinOS 9.1 <version> BIOS package <version>—for your thin client model and click the download icon.

   For information about BIOS installation, see BIOS Installation.

6

Add ThinOS firmware to the Wyse Management Suite repository

Steps

1. Log in to Wyse Management Suite using your tenant credentials.
2. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS**.
3. Click **Add Firmware file**.
   The **Add File** screen is displayed.
4. To select a file, click **Browse** and go to the location where your file is located.
5. Enter the description for your file.
6. Select the check box if you want to override an existing file.
7. Click **Upload**.

   NOTE: The uploaded firmware can be used only to upgrade ThinOS 8.6 to ThinOS 9.1. The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy firmware to a device or a group of devices, go to the respective device or group configuration page.

7

Upgrade ThinOS 8.6 to ThinOS 9.1

ThinOS 9.1 conversion is a two-step process that upgrades your existing ThinOS 8.6 thin client using a **ThinOS** policy for 8.6, and after the upgrade is complete, use a **ThinOS 9.x** policy to manage your ThinOS 9.1-based thin clients. Dell Technologies recommends that you upgrade to ThinOS 9.1 from ThinOS 8.6_606 or later versions.

Prerequisites

- The ThinOS conversion image must be added to the ThinOS firmware repository. For more information, see Add ThinOS firmware to the repository.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered 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**.
   The **Select ThinOS Configuration Mode** window is displayed.
3. Select **Advanced Configuration Mode**.
4. Go to **Firmware Upgrade**, and click **Configure this item**.
5. Clear the **Disable Live Upgrade** and **Verify Signature** check boxes.
6. From the **Platform Type** drop-down list, select the platform.
7. From the **Firmware to auto-deploy** drop-down list, select the firmware added to the repository.
8. Click **Save & Publish**.
   The firmware is deployed to the thin client. The conversion process takes around 10 minutes, and the thin client restarts automatically.

   NOTE: The download of the ThinOS 9.1 image from Wyse Management Suite (both private and public cloud) to the thin client takes around nine minutes depending on the network bandwidth or cloud server performance. The device reboots after the ThinOS image has been downloaded. After the upgrade is complete, the device is automatically registered to Wyse Management Suite.

   NOTE: Make sure that the 5070 BIOS version is 1.3.1 or later before upgrading to ThinOS 9.1. If you upgrade to ThinOS 9.1 with earlier BIOS version and then upgrade the BIOS version to 1.3.1 or later, it may fail to boot up the devices.

   NOTE: You can add the ThinOS policy with ThinOS 8.6 to ThinOS 9.1.1131 base image and ThinOS 9.x policy with ThinOS 9.x operating system image in the same group. This will enable you to upgrade from ThinOS 8.6 to ThinOS 9.x or later versions directly.

Upgrade ThinOS 9.x to later versions

Prerequisites

- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.
- Ensure you have downloaded the latest version of the ThinOS 9.x operating system image.

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 operating system firmware option under the Standard tab, use the Advanced tab.

5. Click **Browse** and select the ThinOS 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 and restarts. The firmware version is upgraded.

   NOTE: If upgrade from ThinOS 9.0 to 9.1, it is recommended to upgrade the OS image before proceeding further. After upgrading to 9.1, install application packages. If the OS image and application packages are in the same WMS group to upgrade. ThinOS 9.0 downloads and installs the application packages even before installing the OS image. After upgrading to ThinOS 9.1, all the existing application packages are cleared, and then the application packages are downloaded and installed again. If you add many application packages with OS image in the same WMS group, the upgrade may fail due to low disk space. If the upgrade fails due to low disk space, then you must reset to factory settings to initiate the upgrade.

   NOTE: Make sure that the 5070 BIOS version is 1.3.1 or later before upgrading to ThinOS 9.1. If you upgrade to ThinOS 9.1 with earlier BIOS version and then upgrade the BIOS version to 1.3.1 or later, it may fail to boot up the devices.

Upload and push ThinOS 9.1 application packages

ThinOS 9.1 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. From the **Select ThinOS Package(s) to deploy** drop-down menu, select the package.

   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**.

8

Configuring a ThinOS 9.1 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 9.1

The following is an overview of the major device configuration changes between ThinOS 8.6 and ThinOS 9.1 that simplifies the configuration process:

Table 7. Configuration comparisons between ThinOS 8.6 and ThinOS 9.1

ThinOS 8.6	ThinOS 9.1
ThinOS 8.6 requires INI files with complex parameter syntax to configure devices.	ThinOS 9.1 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 9.1 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 9.1 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 8. ThinOS configuration grouping overview

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

Table 8. ThinOS configuration grouping overview (continued)

Group Types	Configurations
	Management Settings 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 9. 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.
$DHCP (extra_dhcp_option)	For example, set a string test169 for option tag 169 in DHCP server, and set TerminalName=$DHCP(169) in the Wyse Management Suite server. After the thin client checks in to the Wyse Management Suite server, check the terminal name in GUI, and the terminal name is changed to test169. 166 and 167 is default for CCM MQTT Server and CCM CA Validation in ThinOS. So you need to remap the options from GUI if you want to use $DHCP(166) and/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 with xxx.xxx.xxx.xxx, for example,123.123.123.022.

Table 9. ThinOS system variables

Variable	Description
$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.

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 10. Relationship between INI and Wyse Management Suite group-based configurations (continued)

Configuration	ThinOS 8.6 with INI	ThinOS 9.1 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 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)	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. **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)	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 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**. Select Group feature is not supported by Wyse Management Suite Device Policy Child Groups.	SelectGroup parameter (WNOS\INI\GROUPS)	Groups and Configs Device Policy Parent Group with Select Group Enabled

Table 10. Relationship between INI and Wyse Management Suite group-based configurations

Configuration	ThinOS 8.6 with INI	ThinOS 9.1 with Wyse Management Suite
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 9.1 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. Additionally, a user configuration payload is received at Login.

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

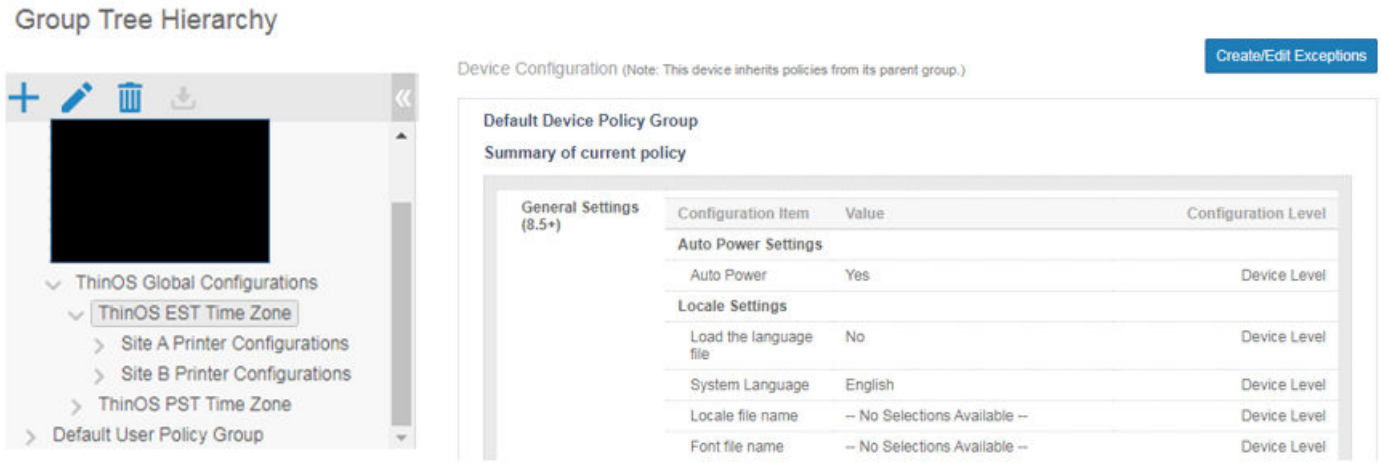

Figure 1. Device policy

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

- Ensure that you have downloaded the BIOS file from Dell.com/support to your device.
- Ensure that you have registered the thin client to Wyse Management Suite, if you are upgrading BIOS using Wyse Management Suite.

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: When you use the BIOS upgrade feature for the first time, the BIOS is downloaded even if the existing BIOS version is the same version that is uploaded.

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.
- 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, enable or disable the MAC Address Pass-Through feature. This option is applicable only to the Wyse 5470 Thin Client.
8. Click **Save & Publish**.

   NOTE: If the BIOS does not have a password and if you are setting a new password, then the password is applied after the first reboot. Other setting changes are applied after the second reboot.

10

Delete ThinOS application packages

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

About this task

This section describes steps to delete ThinOS packages using the ThinOS local UI.

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, see the latest *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.