Windows 10 IoT Enterprise LTSC 2021

Deployment Guide

October 2024
Rev. A02

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 to Windows 10 IoT Enterprise LTSC 2021

Windows 10 IoT Enterprise LTSC 2021 provides a secure way for devices requiring reliable access to applications, files, and network resources. Designed for remote management and administration, this operating system provides a familiar Windows interface for users while ensuring a secure environment.

Key features of Windows 10 IoT Enterprise LTSC 2021 include:

- **Remote access**—Enables users to connect to desktops or virtual environments from various devices.
- **Local administration**—Supports on-device management and maintenance tasks.
- **Customization**—Offers optional add-ons to expand functionality and compatibility.
- **Security**—Provides a secure 64-bit environment for specialized applications.

Audience

This guide is intended for administrators responsible for managing devices running Windows 10 IoT Enterprise LTSC 2021, specifically those using Dell Technologies operating system images.

ⓘ **NOTE:** It is assumed that you are logged in as an administrator when configuring the operating system or using administrative applications.

Document purpose

This document provides instructions for logging into Windows 10 IoT Enterprise LTSC 2021 devices and conducting proof-of-concept tests using Wyse Management Suite for application deployment and configuration management.

2

Getting started with Windows 10 IoT Enterprise LTSC 2021

The automatic activation feature of Windows 10 IoT Enterprise LTSC 2021 ensures secure operation immediately upon connecting your device to the Internet.

For effective device management, Dell Technologies recommends Wyse Management Suite (WMS). WMS offers a centralized approach, allowing you to:

- Configure, monitor, manage, and optimize all devices from a single location.
- Automate tasks, saving IT time and resources as your deployment grows.
- Reduce management costs for large deployments.
- Secure connections with HTTPs-based communications, two-factor authentication, and roles-based provisioning.
- View alerts, receive notifications, and send remote commands to devices.

Wyse Device Agent (WDA) is installed on the device to enable IT administrators to manage the devices through WMS. WDA is a unified agent for device management solutions.

NOTE: Devices are also compatible with other management solutions such as Microsoft Endpoint Configuration Manager and VMware Workspace One.

Logging in to the device

Upon startup, the device will automatically log in to the User desktop. If you want to access the device with a different user account, sign out of the current account and select the preferred user account from the login screen.

The default credentials for different user types are:

- **Administrators**
  - Username—**`Admin`**
  - Password—**`Admin#<Service Tag of the device>`**. For example, if the Service Tag of the device is 1X630C1, the password is **`Admin#1X630C1`**.
- **Users**
  - Username—**`User`**
  - Password—**`User#<Service Tag of the device>`**. For example, if the Service Tag of the device is 1X630C1, the password is **`User#1X630C1`**.

NOTE: For information about how to find the Service Tag of the device, see Find your Service Tag or Serial Number.

Before configuring your device

Before configuring your device, it is important to manage the Unified Write Filter (UWF). The UWF prevents changes that are made to the device from persisting across reboots. To apply permanent configuration changes, you must disable the UWF before making modifications. Once the configuration is complete, enable the UWF. For information about configuring the UWF, see the *Unified Write Filter* section in the *Windows 10 IoT Enterprise LTSC 2021 Administrator's Guide* at Dell | Support.

3

Using Wyse Management Suite

Wyse Management Suite (WMS) provides a centralized platform for managing your devices. Leveraging the Wyse Device Agent (WDA), WMS offers efficient device management features. To enhance device functionality, the Dell Application Store provides a range of pre-packaged applications that can be deployed through WMS.

Wyse Management Suite versions

Wyse Management Suite (WMS) is available in two editions: Standard and Pro.

- **Standard (Free)**—Ideal for small and medium businesses with on-premises deployments, WMS Standard provides basic functionalities. To activate it, you require a license key that is generated from the Wyse Management Suite trials page. Support for this edition is limited to manuals and videos available on Dell | Support.
- **Pro (Paid)**—Ideal for both cloud and on-premises environments, WMS Pro provides advanced management functionalities. It uses subscription-based licenses and allows for hybrid cloud deployment with floating licenses between cloud and on-premises infrastructure. Also, WMS Pro provides technical support for troubleshooting any issues that you encounter.

Create device policy group in WMS

You can create groups in WMS to define the policies that are required to configure your devices. You can create subgroups to further categorize devices based on their function or type. If the configuration policies are not defined for the subgroup, then the configurations of the parent group are inherited by the subgroup.

Steps

1. Log in to WMS as an administrator.
2. Go to the **Groups & Configs** page and click **Default Device Policy Group**.
3. Click the + icon to add a new group.
4. In the **Add New Group** dialog box, enter the group name and description.
5. In the **Registration** tab, select the **Enabled** checkbox under **Group Token**.
6. Enter a group token.

   A group token is a unique identifier that is required to register the devices to a group.
7. Click **Save**.

   The group is added to the list of available groups on the **Groups & Configs** page.

Register devices to WMS

You can register the devices to WMS using any of the following methods:

- Manually using the Wyse Device Agent application on the device.
- Using DNS record fields or DHCP scope options. See, Registering devices by using DHCP option tags and Registering devices by using DNS SRV record.
- Using secure DNS record fields or DHCP scope options. See, Register devices using secure DNS record fields or secure DHCP scope options.

WMS provides the **Enrollment Validation** feature, which allows administrators to control which devices are automatically or manually added to specific groups. This feature is enabled by default and allows administrators to:

- View the registration status of the devices displayed as **Pending** on the **Devices** page. You can filter the devices using the **Enrollment Validation Pending** status filter.
- Review and validate individual devices or select multiple devices for validation.

- Once validated, the devices are assigned to their designated group.

For more information about how to validate the devices, see Enrollment Validation.

When the **Enrollment Validation** option is disabled, the device is directly assigned to the designated group.

Register devices using Wyse Device Agent

Prerequisites

Create a group and a group token in WMS. For information about how to create a group, see Create a device policy group in Wyse Management Suite.

Steps

1. Log in to the device as an administrator.
2. Open the Wyse Device Agent application located in the **System Tray**.
   The **Wyse Device Agent** screen is displayed.
3. From the **Management Server** drop-down list, select **Wyse Management Suite**.
4. Enter the appropriate server address and port number for your data center:
   - If you are using the WMS cloud environment:
     - **US data center**—us1.wysemanagementsuite.com
     - **EU data center**—eu1.wysemanagementsuite.com

     The default port number is 443.
   - If you are using the WMS on-premises environment, enter the on-premises FQDN address and the custom port number.

   NOTE: If the server address contains **http**, a warning message is displayed. Click **Ok** to confirm.
5. Enter the group token in the **Tenant** and **Group** field. For example, if the group token for the group is **`defa-Acme@123`**, enter **`defa`** in the **Tenant** field and **`Acme@123`** in the **Group** field.
6. Enable or disable CA validation.
   If you disable CA validation, a warning message is displayed. Click **Ok** to confirm.

   NOTE: For the cloud environment of WMS, CA validation must be enabled.
7. Click **Register** to complete the process.

4

Dell Application Store

The Dell Application Store is a software bundle consisting of Dell value-added applications. The following applications are bundled in the Dell Application Store:

- **Wyse Device Agent (WDA)**
  - Description—Enables you to quickly and easily deploy configurations on devices.
  - Benefits—Allows you to manage devices using WMS.
- **Wyse Easy Setup**
  - Description—Enables you to quickly and easily deploy configurations on devices.
  - Benefits—Create a kiosk mode to lock down a Windows device, preventing users from accessing any features outside of the kiosk mode. Customize the kiosk interface to control user access to specific features.
- **Dell Application Control Center**
  - Description—Offers a user interface to manage device configurations, embedded applications, and utilities.
  - Benefits—Provides a kiosk mode with centralized management capabilities.
  - **Application Launch Manager**
    - Description—Enables you to start any application based on predefined events (service startup, user logoff, or device shutdown). Application Launch Manager is configurable only using the Dell Application Control Center user interface.
    - Benefits—Configure multilevel logs essential for troubleshooting.
  - **Extra Data Cleanup Manager**
    - Description—Keeps extraneous information from being stored on the local disk. Extra Data Cleanup Manager is configurable only using the Dell Application Control Center user interface.
    - Benefits—Automatically cleans up directories that are used for temporary caching of information, triggered by service startup, user logoff, or device shutdown. This clean-up is invisible to the user and configurable.
- **Overlay Optimizer**
  - Description—Works with Microsoft Unified Write Filter (UWF).
  - Benefits—Provides write protection and extends device uptime by monitoring UWF overlay space and moving unused content to the overlay of Overlay Optimizer disk.

NOTE: Overlay Optimizer runs in the background, and you cannot configure it.

To deploy the software bundle to the devices using WMS, see Deploy applications using WMS.

If you are using the WMS cloud, the latest Dell Application Store can be deployed directly from the cloud. To view the packages in WMS cloud, go to **Apps & Data** > **App Inventory** and select **Operator Cloud WMS** from the **File respository** drop-down menu.

If you are using the Wyse Management Suite on-premises environment, you must download the latest Dell Application Store package (DellApplicationStore_xx.xx.x.x.exe) from the respective hardware landing page on Dell Support and upload to the repository. To upload the files to the repository, see How to add an application package to the WMS repository.

After the successful deployment of the package, to verify the version details of the Dell Application Store and the installed components of Dell Application Store such as DACC, WDA, ALM, and so on, do any of the following:

- On the device, open **Dell Application Control Center** and verify the version details.
- Log in to Wyse Management Suite and go to **Devices** > **<Device Details page of the individual device>** > **Installed Apps**.

5

WinIoT 2.x policy in WMS

WMS 4.1 and later versions offer enhanced support for WinIoT 2.x policy through a new user interface. This interface incorporates a search function, allowing users to efficiently locate the required configuration options.

Dell Technologies recommends that you use WinIoT 2.x policy on WMS to configure the devices.

For any device to be recognized as WinIoT 2.x policy-enabled, it requires the installation of ConfigUISupport.exe on the device. This file ensures compatibility with the new policy management features.

To verify if the devices are using the WinIoT 2.x policy in WMS, go to the **Devices** page in WMS and from the **OS Type** filter, select **WinIoT 2.x**.

Prerequisites to enable WinIoT 2.x policy on the device

If you are using the older WinIoT (WES) configurations, you must redo all the configurations after you transition to WinIoT 2.x policy.

The following components must be installed on the device to enable the WinIoT 2.x policy:

- Wyse Device Agent 14.6.9.x or later versions
- Wyse Easy Setup 2.0.0.471 or later versions
- **Windows 10 IoT Config UI Enabler Package** (`ConfigUISupport_1.0.0.8.exe`)

For the WMS cloud, `ConfigUISupport_1.0.0.8.exe` package is already added to the **App Inventory** in the **Apps & Data** page of WMS.

For the WMS on-premises environment, you must download the latest **Windows 10 IoT Config UI Enabler Package** (`ConfigUISupport_1.0.0.8.exe`) from the respective hardware landing page on Dell | Support and upload to the repository. To upload the files to the repository, see How to add an application package to the WMS repository.

To deploy the package to the devices using WMS, see Deploy an application using WMS.

ⓘ **NOTE:** You must use the silent installation parameter **`--silent`** when you are deploying the **Windows 10 IoT Config UI Enabler Package** from WMS.

Edit the WinIoT 2.x policy settings in WMS

Steps

1. Log in to WMS as an administrator.
2. Go to the **Groups & Configs** page and select a group.
3. From the **Edit Policies** drop-down menu, click **WinIoT 2.x**.
   The **Configuration Control | WinIoT 2.x** window is displayed.
4. Click **Advanced**.
5. In the respective fields, click the option that you want to configure.

   You can use the search field at the top of the page to locate specific settings. The search result displays the settings in the following order:

   - Setting
   - Parameter Group
   - Parameter subgroup
   - Parameter
6. Configure the options as required.

ⓘ **NOTE:** You can click the **Reset Policy** option to reset the policy to default configurations. You can also click the **Reset Entire Policy** option if you want to clear all configurations.

7. Click **Save & Publish**.

ⓘ **NOTE:** The policy configurations with reference files, such as firmware, package, wallpaper, and so on, applied to the parent group are inherited by default to the child groups. You can override these configurations for the child groups.

Unified Write Filter (UWF) Servicing Mode

Microsoft provides various updates, which are categorized as important, recommended, and optional. These updates offer significant advantages, including enhanced security and improved device reliability.

During normal operations, with the UWF enabled, device updates are automatically disabled as they would be discarded upon device reboot due to the UWF overlay clearing. The UWF Servicing Mode allows you to schedule a job for planned automatic critical Windows Updates and antimalware signature files.

When UWF Servicing Mode is triggered,

- The operating system reboots the device, clearing the UWF overlay and temporarily disables the write filter.
- A designated maintenance window opens, providing a dedicated time for update installation.
- The device scans for and applies any necessary Windows Updates within the maintenance window.
- The device enters a locked state. You must not enter any keys or enter any password when the **UWF-Servicing** screen is displayed.

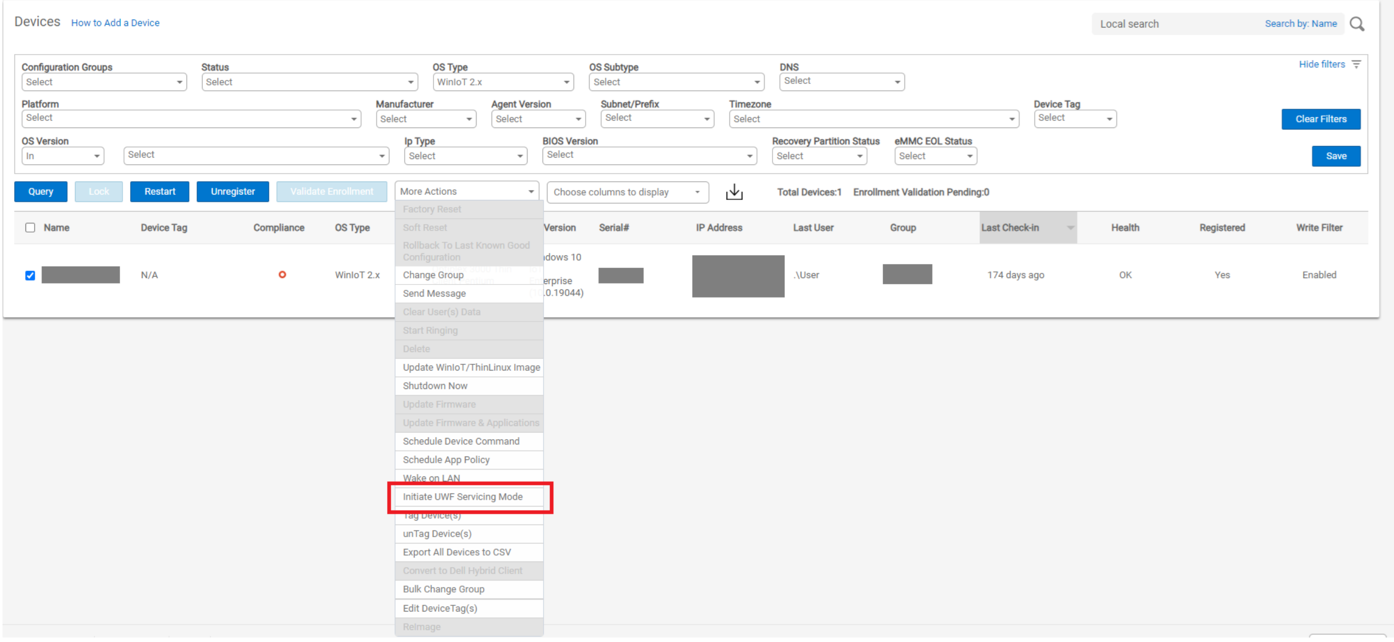
NOTE: The devices require an unauthenticated Internet connection to update the devices using UWF Servicing Mode.

Initiate UWF Servicing Mode manually from WMS

The UWF Servicing Mode can be triggered manually from the WMS server for a single device or multiple devices.

Steps

1. Log in to WMS as an administrator.
2. Go to the **Devices** page.
3. Apply the filters to find the preferred devices.
4. Select the checkbox of the device or devices.
5. From the **More Actions** drop-down menu, click **Initiate UWF Servicing Mode**.



Configuration Groups: Select
Status: Select
OS Type: WinIoT 2.x
OS Subtype: Select
DNS: Select
Platform: Select
Manufacturer: Select
Agent Version: Select
Subnet/Prefix: Select
Timezone: Select
Device Tag: Select
OS Version: In | Select
Ip Type: Select
BIOS Version: Select
Recovery Partition Status: Select
eMMC EOL Status: Select

Total Devices:1 Enrollment Validation Pending:0

☐ Name	Device Tag	Compliance	OS Type	Version	Serial#	IP Address	Last User	Group	Last Check-in	Health	Registered	Write Filter
☑ [redacted]	N/A	○	WinIoT 2.x	dows 10 erprise 0.19044)	[redacted]	[redacted]	.\User	[redacted]	174 days ago	OK	Yes	Enabled

Figure 1. Initiate UWF Servicing Mode

An alert window is displayed.

6. Click **Send Command** to initiate the UWF Servicing Mode to the selected devices.

   ⓘ **NOTE:** The UWF Servicing Mode can also be triggered in the same manner from the **Device Details** page.

Schedule a UWF Servicing Mode job from WMS

You can set up a recurring device command to run UWF Servicing Mode regularly on the selected devices.

Steps

1. Log in to WMS as an administrator.
2. Go to the **Jobs** page.
3. Click **Schedule Device Commands**.
4. From the **Command** drop-down menu, select **Initiate UWF Servicing Mode**.
5. From the **OS Type** drop-down menu, select **WinIoT**.
6. Enter a name for the job.
7. Select the group for which you want to schedule the device command job.
8. Enter the job description.
9. From the **Run** drop-down list, select any of the following options:
   - **Immediately**
   - **On selected time zone and date/time**
   - **On selected date/time**
10. Select the time zone if you have selected **On selected time zone and date/time** in Step 9.
11. Enter or select the following details if you have selected **On selected time zone and date/time** or **On selected date/time** in Step 9:
    - **Effective**—Enter the starting and ending date.
    - **Start between**—Enter the starting and ending time.
    - **On day(s)**—Select the days of the week.
12. Click the **Preview** option to view the details of the scheduled job.
13. On the next page, click the **Schedule** option to initiate the job.

Results

You can verify the status of the job from the **Jobs** page.

Deploy third-party applications for Windows 10 IoT Enterprise LTSC 2021

You can deploy third-party applications and VDI plugins on Windows 10 IoT Enterprise LTSC 2021 devices using WMS. You can download the following individual third-party applications as add-ons from the Dell | Support page.

- VMware Horizon Client
- Citrix Workspace app
- Amazon WorkSpaces
- Cisco Jabber Softphone for VDI (Virtual Desktop Infrastructure) Client
- Cisco Webex App VDI Plugin (Bundled Webex Meetings VDI plugin)
- Zoom VDI Universal plugin

To deploy the package to the devices using WMS, see Deploy an application or a package using Wyse Management Suite.

If you are using the WMS cloud, the latest available application package can be deployed directly from the cloud. To view the packages in WMS cloud, go to **Apps & Data** > **App Inventory** and select **Operator Cloud WMS** from the **File respository** drop-down menu.

If you are using the Wyse Management Suite on-premises environment, you must download the latest application package from the respective hardware landing page on Dell | Support and upload to the repository. To upload the files to the repository, see How to add an application package to the WMS repository.

After the successful deployment of the package, to verify the version details of the installed components, log in to WMS and go to **Devices** > **Device Details page of the individual device** > **Installed Apps**.

8

Deploy driver packages for Windows 10 IoT Enterprise LTSC 2021

You can deploy and install driver packages on Windows 10 IoT Enterprise LTSC 2021 devices using WMS.

Steps

1. Locate the required driver package:
   a. Go to Dell | Support and identify the device.
   b. On the **Drivers & Downloads** page, use the following options to locate and download the driver:
      - **Keyword**
      - **Operating System**—Select **Windows 10 IoT Enterprise LTSC 2021** from the drop-down list.
      - **Download Type**—Select **Driver** from the drop-down list.
      - **Category**—Select the options as required.
2. Download the necessary driver files.
3. Upload the downloaded driver files to the WMS repository. For information about how to upload the driver files to the WMS repository, see How to add an application package to the WMS repository.
4. Deploy the package to the devices using WMS. For information about how to deploy an application or package using WMS, see Deploy an application or a package using WMS.

   ⓘ **NOTE:** For information about the silent installation parameters for the drivers, see How to find the silent installation parameters of third-party drivers.

9

Deploy applications using WMS

To deploy multiple applications to different subgroups, use the **Advanced App Policy** feature in WMS. This functionality is available only in the Pro edition of WMS.

Prerequisites

You must upload the application and the pre or post install scripts (if necessary) to the **App Inventory**. To upload the files:

1. Log in to WMS as an administrator.
2. Go to **Apps & Data** > **App Inventory** > **Thin Client** and click **Add WinIoT Package file** to upload the application and the pre or post-install scripts (if necessary).

    ⓘ **NOTE:** The **App Inventory** interface may take up to two minutes to display newly added programs.

Steps

1. Go to **Apps & Data** > **App Policies** > **Thin Client**.
2. Click **Add Advanced Policy**.
   The **Add Advanced App Policy** page is displayed.
3. Enter the **Policy Name**.
4. From the **Group** drop-down list, select one or more groups to which you want to deploy the application.
5. Select the **Include All Subgroups** checkbox to apply the policy to subgroups.
6. From the **Task** drop-down list, select **Install Application**.
7. From the **OS Type** drop-down list, select **WinIoT**.
8. Select the **Filter files based on extensions** checkbox to filter the applications. If you select this option, only the applications that are associated with the selected operating system type are displayed.
9. From the **Filter Devices** drop-down list, select any of the following options:
   - Select the **Apply On All Devices** option if you want to apply the policy to all the devices.
   - Select the **Filter already updated devices** option if you do not want the previously deployed applications using WMS to be redeployed.
   - Select the **Filter devices with policy already applied** if you do not want to apply the policy to devices which have already received the same policy.
10. Click **Add app**.

    From the **Apps (applied in the order shown.)** drop-down list, select an application. Optionally, select the pre and post-install script under **PreInstall**, **PostInstall**, and enter the **Install Parameters**.

    The following table lists the Dell value-added applications and Dell Technologies-supported third-party applications which are available as individual add-on packages at Dell | Support and their respective silent installation parameters:

Table 1. Dell value-added applications and Dell Technologies-supported third-party applications

Application name	Silent installation parameters
Dell Application Store	--silent
Wyse Device Agent	--silent
VMware Horizon Client	--silent
Citrix Workspace app	--silent
Amazon WorkSpaces	--silent
Cisco Jabber Softphone for VDI (Virtual Desktop Infrastructure) Client	/qn

Table 1. Dell value-added applications and Dell Technologies-supported third-party applications (continued)

Application name	Silent installation parameters
Cisco Webex App VDI Plugin (Bundled Webex Meetings VDI plugin)	/qn
Zoom VDI Universal plugin	/quiet /norestart

> **NOTE:** Dell Application Store, Wyse Device Agent, VMware Horizon Client, Citrix Workspace App, and Amazon WorkSpaces support silent installation (no installation parameter is required) from WMS if Wyse Device Agent version 14.6.9.26 or later is installed on the device.

11. To stop the installation process after a defined value, specify the number of minutes in the **Install Timeout** field. The default value is 60 minutes.
12. If you want the device to reboot after the application is successfully installed, select **Reboot**.
13. Click **Add app** and repeat the step to add multiple applications.
14. Select **Enable app dependency** to stop the application policy at first failure.
15. From the **OS Subtype Filter**, select **WIE10 (Windows 10 IoT Enterprise)**.
16. From the **Platform Filter**, select the device model to which you want to deploy the application.
17. In the **Timeout** field, enter the number of minutes the message dialog box should be displayed on the device, which gives you time to save your work before the installation begins.
18. To enable delay in the implementation of the policy for the user, select the **Allow delay of policy execution** checkbox. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay running the policy.
    - From the **Max delays** drop-down list, select the number of times (1–3) you can delay running the policy.
19. From the **Apply Policy Automatically** drop-down list, select any of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.
20. Select the **Skip write filter check** checkbox if you want to configure a setting with the write filter enabled.

    This option is enabled if the **Enable app dependency** option is enabled. Also, the option is applied only if the policy is applied using a job.
21. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
22. Select **Yes** to schedule a job on the same page or select **Later** to schedule the job later.
23. If you selected **Yes** in step 22, select any of the following options:
    - **Immediately**—The server runs the job immediately.
    - **On device time zone**—The server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—The server creates one job to run at the date or time of the designated time zone.
24. To create the job, click **Preview** and schedules are displayed on the next page.

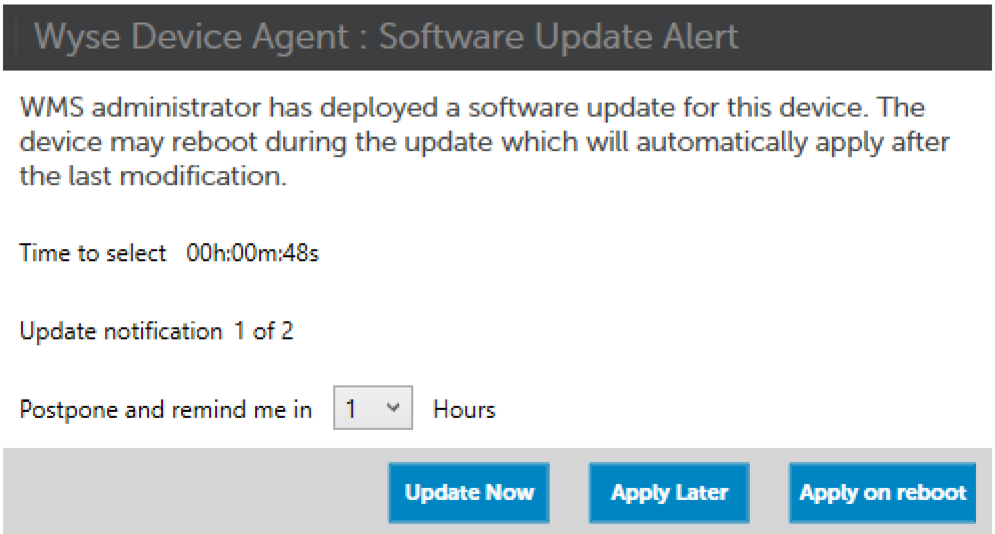
    For more information about scheduling a job, see Schedule an application policy.

Results

You can check the status of the job by going to the **Jobs** page.

Next steps

On the device, **Wyse Device Agent : Software Update Alert** window is displayed.



Wyse Device Agent : Software Update Alert

WMS administrator has deployed a software update for this device. The device may reboot during the update which will automatically apply after the last modification.

Time to select 00h:00m:48s

Update notification 1 of 2

Postpone and remind me in 1 Hours

Figure 2. Wyse Device Agent : Software Update Alert

You can postpone the execution of the policy that is based on the configurations in step 18. The following details are displayed:

- **Time to select**—The time before which you must select an option on the screen.
- **Update notification**—Displays the number of times that you can defer the update.
- **Postpone and remind me in**—Select the time in hours that you want to postpone the update and an alert window to be displayed again on the device.

You can also select any of the following options:

- **Update Now**—Click this option to apply the update immediately.
- **Apply Later**—Click this option to apply the update later.
- **Apply on Reboot**—Click this option to apply the update when you reboot the device.

Schedule application policy

Steps

1. Log in to WMS as an administrator.
2. On the **Jobs** page, click the **Schedule App Policy** option.
   The **App Policy Job** screen is displayed.
3. From the drop-down list, select the application policy that you want to schedule.
4. Enter the job description.
5. From the **Run** drop-down list, select any of the following options:
   - **Immediately**
   - **On selected time zone and date/time**
   - **On selected date/time**
6. Select the **Exclude Offline Devices** if you want to exclude the offline devices while creating the job.
   You can view the list of excluded offline devices on the **Jobs** page. You can later restart the job for the offline devices from the jobs list.
7. Select the time zone if you have selected **On selected time zone and date/time** in Step 4.
8. Enter or select the following details if you have selected **On selected time zone and date/time** or **On selected date/time** in Step 4:
   - **Effective**—Enter the starting and ending date.
   - **Start between**—Enter the starting and ending time.
   - **On day(s)**—Select the days of the week.
9. Click the **Preview** option to view the details of the scheduled job.
10. On the next page, click the **Schedule** option to initiate the job.

10

Frequently asked questions

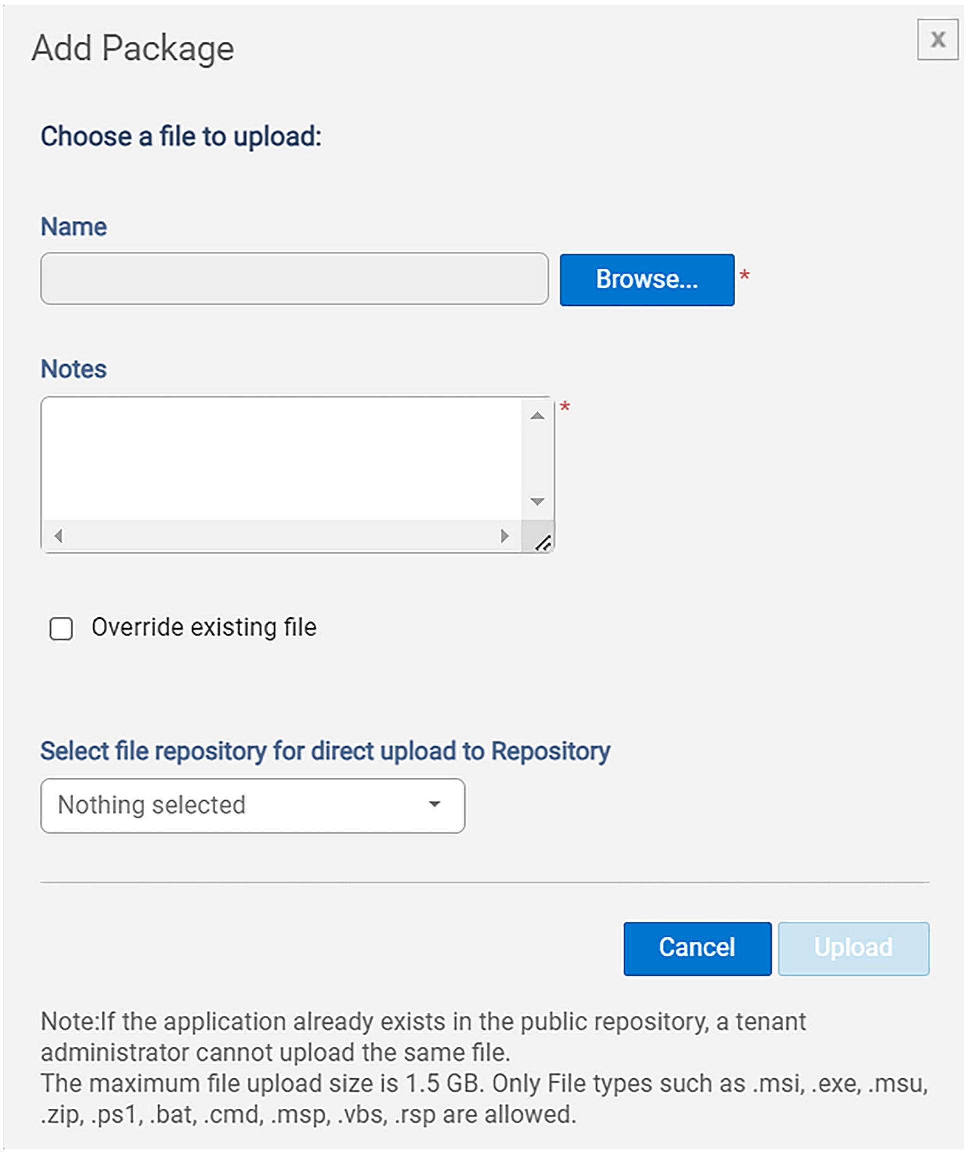
How to add an application package to the WMS repository?

Prerequisites

- For the on-premises environment, download and install the WMS remote repository. To download the repository, log in to Wyse Management Suite as an administrator, go to **Portal Administration** > **File Repository** and use the download link.
- Download the application packages from Dell | Support for the respective device.

Steps

1. Log in to WMS as an administrator.
2. Go to **Apps & Data**.
3. Click **Add WinIoT Package file**.
   The **Add Package** window is displayed.



Note:If the application already exists in the public repository, a tenant administrator cannot upload the same file.
The maximum file upload size is 1.5 GB. Only File types such as .msi, .exe, .msu, .zip, .ps1, .bat, .cmd, .msp, .vbs, .rsp are allowed.

Figure 3. Add WinIoT Package file

4. Browse to the location where you have downloaded the application package.
5. In the **Notes** field, add information about the package.
6. Select the **Override existing file** option if you want to replace the existing application package.
7. From the **Select file repository for direct upload to Repository** drop-down list, select the repository to which you want to upload the application package.
8. Click **Upload**.

> **NOTE:** For the on-premises environment, you can also directly place the application package files to `<repo-dir>\repository\thinClientApps` on the device, and the repository sends metadata for all the files to the server periodically.

How to find the silent installation parameters of third-party drivers

Steps

1. Open **Command Prompt** as an administrator.
2. Locate the driver executable file and add **`/?`** or **`--help`**.

3. Press **Enter**.
   The silent installation parameters (if any) are displayed.