

# Windows 11 IoT Enterprise LTSC 2024

## Deployment Guide

## Notes, cautions, and warnings

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

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

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

<b>Chapter 1: Introduction to Windows 11 IoT Enterprise LTSC 2024.....</b>	<b>4</b>
Audience.....	4
Document purpose.....	4
<b>Chapter 2: Getting started with Windows 11 IoT Enterprise LTSC 2024 .....</b>	<b>5</b>
Logging in to the device.....	5
Before configuring your device.....	5
<b>Chapter 3: Using Wyse Management Suite.....</b>	<b>6</b>
Wyse Management Suite versions.....	6
Create device policy group in Wyse Management Suite.....	6
Register devices to Wyse Management Suite.....	6
Register devices using Wyse Device Agent .....	7
<b>Chapter 4: Dell value-added applications.....</b>	<b>8</b>
<b>Chapter 5: Windows Updates with UWF Servicing Mode.....</b>	<b>9</b>
Schedule a UWF Servicing Mode job from WMS.....	9
Initiate UWF Servicing Mode manually from WMS.....	10
<b>Chapter 6: Deploying updates for Microsoft Edge using WMS.....</b>	<b>11</b>
<b>Chapter 7: Deploying third-party applications for Windows 11 IoT Enterprise LTSC 2024.....</b>	<b>12</b>
<b>Chapter 8: Deploying driver packages for Windows 11 IoT Enterprise LTSC 2024.....</b>	<b>13</b>
<b>Chapter 9: Deploying applications using WMS.....</b>	<b>14</b>
Schedule an application policy.....	16
<b>Chapter 10: Frequently asked questions.....</b>	<b>18</b>
How to find and download any package on Dell support?.....	18
How to add an application package to the WMS repository?.....	18
How to find the silent installation parameters of drivers and application packages.....	19

# Introduction to Windows 11 IoT Enterprise LTSC 2024


Devices with Windows 11 IoT Enterprise LTSC 2024 provide a secure and reliable way to access applications, files, and network resources. This operating system enables remote management and administration, using the familiar Windows interface to ensure a secure environment for users.

Key features of Windows 11 IoT Enterprise LTSC 2024 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 deployment guide is intended for administrators responsible for managing devices running Windows 11 IoT Enterprise LTSC 2024, 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

The document details the steps for getting started with Windows 11 IoT Enterprise LTSC 2024 using Wyse Management Suite to deploy applications and manage configurations.


# Getting started with Windows 11 IoT Enterprise LTSC 2024

Devices with Windows 11 IoT Enterprise LTSC 2024 activate automatically and ensure secure operation when connected to the Internet.

For effective device management, it is recommended to use 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 pre-installed on the device to enable IT administrators to manage the devices and deploy configurations through WMS.


 **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 automatically logs 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>**. Replace <Service Tag of the device> with the service tag for your 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>**. Replace <Service Tag of the device> with the service tag for your 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 11 IoT Enterprise LTSC 2024 Administrator's Guide* at [Dell | Support](#).

# 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.

## NOTE:

- WMS 5.0 is required to manage Windows 11 IoT Enterprise LTSC 2024 devices.
- WinIoT 2.x policy manages Windows 11 IoT Enterprise LTSC 2024 devices by default.

## 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 Wyse Management Suite

You can create groups in Wyse Management Suite (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 (Add Group) 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** to create a group token.

 **NOTE:** A random group token is generated when the **Enabled** checkbox under the **Group Token** is cleared.

6. Enter a group token. For example, **defa-Acme@123**.  
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 Wyse Management Suite

You can register the devices to Wyse Management Suite (WMS) using any of the following methods:

- Manually using the Wyse Device Agent application on the device. For more information, see [Register devices using Wyse Device Agent](#).
- Using DNS record fields or DHCP scope options. For more information, 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. For more information, 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. As an administrator you can assign devices to their designated group by following these steps:

- Go to the **Devices** page and select the Status filter as **Enrollment Validation Pending**.
- Select individual devices or multiple devices, then click **Validate Enrollment**.
- After validation, assign the devices 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 Wyse Management Suite (WMS). For information about how to create a group, see [Create 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 **Validate Server Certificate CA**.  
If you disable **Validate Server Certificate CA**, a warning message is displayed. Click **Ok** to confirm.
-  **NOTE:** For the cloud environment of WMS, **Validate Server Certificate CA** must be enabled.
7. Click **Register** to complete the process.  
The status of the registration is displayed in the bottom left corner of the **Wyse Device Agent** screen.

# Dell value-added applications

The Dell value-added applications are as follows:

## Wyse Device Agent (WDA)

**Description**—A unified agent for device management solutions that enables quick and easy deployment of 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**—Administrators can use the interface to locally manage device configurations, Dell value-added applications, and utility tools, providing enhanced control and flexibility.

- **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 (xDCM) 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.

 **NOTE:** Application Launch Manager and Extra Data Cleanup Manager can only be configured from Dell Application Control Center.




# Windows Updates with 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 Unified Write Filter (UWF) enabled, windows 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 disabling the Write Filter (**WF**).
- 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. Do not enter any keys or enter any password when the **UWF-Servicing** screen is displayed.

 **NOTE:** Devices require an Internet connection to update using UWF Servicing Mode.

## 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 (of device time zone)**
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 (of device time zone)** 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.

# 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**.

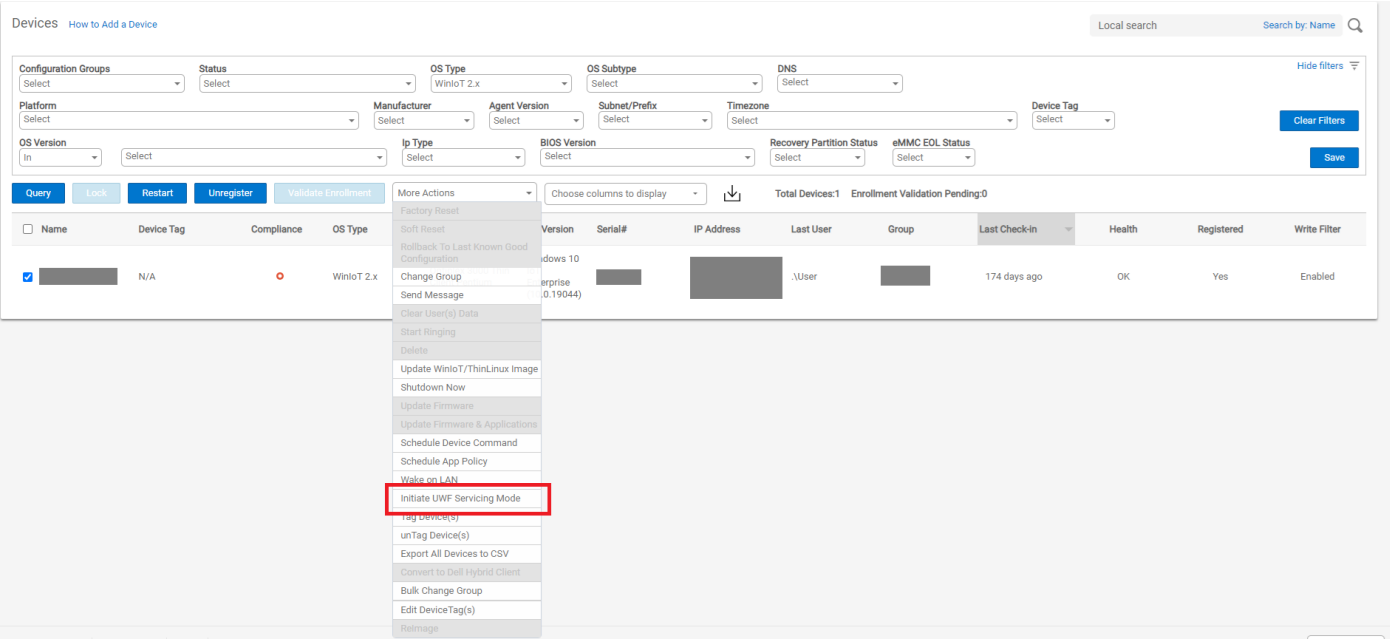


Figure 1. Initiate UWF Servicing Mode



- 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.

# Deploying updates for Microsoft Edge using WMS

Wyse Management Suite (WMS) can be used to install Microsoft Edge updates on supported Windows 11 IoT Enterprise devices. You must download the Microsoft Edge update package from Microsoft Update Catalog, upload the package file to the WMS repository, and deploy it to the WMS group.

## Steps

1. Go to [Microsoft Update Catalog](#).
2. Enter **Microsoft Edge** and click **Search**.
3. Click **Download** to download the Microsoft Edge update package.  
 **NOTE:** It is recommended to download the latest stable channel version of the Microsoft Edge update compatible with x64 processor architecture.
- A **Download** window is displayed.
4. In the **Download** window, click the .cab link and select the location to save the .cab file.
5. Go to the location of the saved .cab file.
6. Right-click the .cab file and **Open with**.
7. Select **Windows Explorer**.  
The .msi file is displayed.
8. Copy the .msi file and go to the desired location in **Windows Explorer** to save it.
9. Upload the .msi file to the WMS repository. For information about how to upload the application package file to the WMS repository, see [How to add an application package to the WMS repository](#).
10. Deploy the package to the devices using WMS. For information about how to deploy an application 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 drivers and application packages](#).

# Deploying third-party applications for Windows 11 IoT Enterprise LTSC 2024

You can deploy third-party applications and VDI plugins on Windows 11 IoT Enterprise LTSC 2024 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 repository** 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**.

# Deploying driver packages for Windows 11 IoT Enterprise LTSC 2024

You can deploy and install driver packages on Windows 11 IoT Enterprise LTSC 2024 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 11 IoT Enterprise LTSC 2024** 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 drivers and application packages](#).

# Deploying applications using WMS

To deploy a single application or multiple applications to different subgroups, use the **Advanced App Policy** feature in WMS. This functionality is available only in the Pro edition of WMS. To deploy a single application to a group, use the **Standard App Policy** feature in WMS. This functionality is available in the Standard 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 postinstall 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 postinstall script under **Pre-Install**, **Post-Install**, and enter the **Install Parameters**.

The following table lists the 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 Technologies-supported third-party applications**

Application name	Silent installation parameters
Cisco Jabber Softphone for VDI (Virtual Desktop Infrastructure) Client	/qn
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 on Windows 11 IoT Enterprise LTSC 2024 devices.

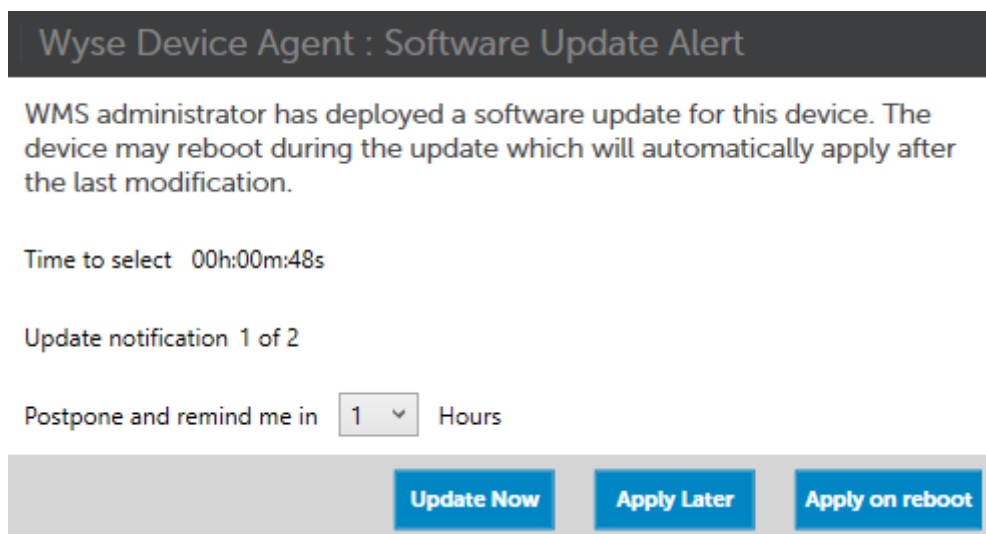
11. To stop the installation process after a defined value, specify the number of minutes in the **Install Timeout** field. The default value is 60 minutes.
12. If you want the device to reboot after the application is successfully installed, select **Reboot**.  
 **NOTE:** It is mandatory to select this option for all the supported third-party applications, such as VMware Horizon Client, Citrix Workspace App, Amazon WorkSpaces, Cisco Jabber Softphone for VDI (Virtual Desktop Infrastructure) Client, Cisco Webex App VDI Plugin (Bundled WebexMeetings VDI plugin), and Zoom VDI Universal plugin.
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 **WIE11 (Windows 11 IoT Enterprise LTSC 2024)**.
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) which 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 skip the write filter cycles.  
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, see [Schedule an application policy](#).
23. If you selected **Yes** in step 22, then an **App Policy Job** window is displayed.
24. In the **App Policy Job** window, select the **Policy**.
25. Enter the description for the job.
26. From the **Run** drop-down list, select any of the following options:
  - **Immediately**
  - **On selected time zone and date/time**
  - **On selected date/time (of device time zone)**
27. 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.
28. Select the time zone if you have selected **On selected time zone and date/time** in Step 26.
29. Enter or select the following details if you have selected **On selected time zone and date/time** or **On selected date/time (of device time zone)** in Step 26:
  - **Effective**—Enter the starting and ending date.
  - **Start between**—Enter the starting and ending time.
  - **On day(s)**—Select the days of the week.
30. Click the **Preview** option to view the details of the scheduled job.
31. On the next page, click the **Schedule** option to initiate the job.

## 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.



**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.

### **NOTE:**

- If you select **Apply Later** in the **Wyse Device Agent: Software Update Alert** notification, the App Policy does not apply immediately, even after shutting down and restarting the device. The App Policy applies based on the user-configured execution delay.
- When you enable the **Allow delay of policy execution** option in WMS and deploy another policy without configuring any delay, the new policy fails to deploy to the device.

## Schedule an application policy

The **Schedule App Policy** option is used to configure the deployment schedule for an existing application policy using Wyse Management Suite.

### 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 (of device time zone)**
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 5.
8. Enter or select the following details if you have selected **On selected time zone and date/time** or **On selected date/time (of device time zone)** in Step 5:
  - **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.

## Frequently asked questions

### How to find and download any package on Dell support?

#### About this task

You can locate a driver, application, BIOSupdate, or any other package from the Dell support site, by following these steps:

#### Steps

1. Go to [Dell | Support](#).
2. Enter the name of the device in **Identify your product or search support**.  
The **Overview** page of the product is displayed.
3. Go to **Drivers & Downloads**.
4. Select **Windows 11 IoT Enterprise LTSC 2024** as the **Operating system**.
5. Select the application or package and click **Download**.  
The file download window is displayed.

### 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.

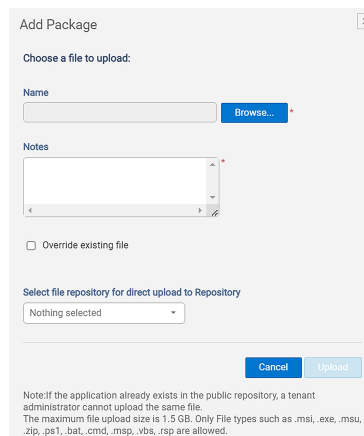


Figure 3. Add WinIoT Package file

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 drivers and application packages

### Steps

1. Open **Command Prompt** as an administrator.
2. Locate the executable file and add `/?` or `--help`.
3. Press **Enter**.  
The silent installation parameters (if any) are displayed.