

# Windows 10 IoT Enterprise LTSC 2021

## 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 10 IoT Enterprise LTSC 2021</b> .....	<b>4</b>
Audience.....	4
Document purpose.....	4
<b>Chapter 2: Getting started with Windows 10 IoT Enterprise LTSC 2021</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>
Create device policy group in Wyse Management Suite.....	6
Register devices to WMS.....	6
Register devices using Wyse Device Agent .....	7
<b>Chapter 4: Dell Application Store</b> .....	<b>8</b>
<b>Chapter 5: WinIoT 2.x policy configurations in Wyse Management Suite</b> .....	<b>9</b>
Prerequisites to enable WinIoT 2.x policy on the device.....	9
Edit the WinIoT 2.x policy settings in WMS.....	9
<b>Chapter 6: Unified Write Filter (UWF) Servicing Mode</b> .....	<b>11</b>
Initiate UWF Servicing Mode manually from WMS.....	11
Schedule a UWF Servicing Mode job from WMS.....	12
<b>Chapter 7: Deploy third-party applications for Windows 10 IoT Enterprise LTSC 2021</b> .....	<b>13</b>
<b>Chapter 8: Deploy driver packages for Windows 10 IoT Enterprise LTSC 2021</b> .....	<b>14</b>
<b>Chapter 9: Deploy application or package using WMS</b> .....	<b>15</b>
Schedule application policy.....	18
<b>Chapter 10: Frequently asked questions</b> .....	<b>19</b>
How to add an application package to the WMS repository.....	19
How to find the silent installation parameters of third-party drivers .....	21

# Introduction to Windows 10 IoT Enterprise LTSC 2021

Devices with Windows 10 IoT Enterprise LTSC 2021 provide a secure and efficient way to access applications, files, and network resources across different machines. This operating system enables users to establish remote connections to desktops or virtual environments, using the familiar Windows interface.

Locally installed software enables both remote administration and essential maintenance tasks directly on the device. Furthermore, optional add-ons expand functionality by accommodating a broader spectrum of peripherals and features that are tailored to specific requirements. Environments necessitating a secure interface with 64-bit Windows compatibility can take advantage of specialized add-ons for optimal performance.

## Audience

This deployment guide is intended for administrators who manage device running the Windows 10 IoT Enterprise LTSC 2021 operating system. It is assumed you are using an operating system image from Dell Technologies and that you log in as an administrator when configuring the operating system or using administrative applications.

## Document purpose

The purpose of this document is to act as a simple guide that outlines the process for logging into devices running Windows 10 IoT Enterprise LTSC 2021 and for proof of concepts involving Wyse Management Suite for application deployment and configuration management.


# 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.
- 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 used to manage the devices using Wyse Management Suite. 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

By default, when you start the device, you are logged in to the user desktop.

To log in with a different user account, you must sign out and click the preferred user account on the login screen. You can use the following credentials to log in to different user accounts:

- **Administrators**—The default username is **Admin** and the default case-sensitive password is **Admin#<Service Tag of the device>**. For example, if the Service Tag of the device is 1X630C1, the password is **Admin#1X630C1**.
- **Users**—The default username is **User** and the default case-sensitive password is **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 you configure your device, ensure that you enable or disable the Unified Write Filter (UWF). If you want the configuration to persist across reboots, you must disable the UWF before configuring the device and enable it again after the device is configured. 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](#).

# Using Wyse Management Suite

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

- **Standard (Free)**—This edition is ideal for small and medium businesses for an on-premises environment. It provides basic functionalities and requires a license key for activation. **Generation of a standard license key**—To generate the key, go to the [Wyse Management Suite trials page](#), select **Start Free WMS Standard**.
- **Pro (Paid)**—This edition is suitable for both cloud and on-premises environment. It requires a subscription-based license key. Advanced management capabilities. Hybrid cloud deployment option, allowing floating licenses between cloud and on-premises environment.


 **NOTE:** Tech support is available only for the WMS Pro edition. For support on the Standard edition, you can see the manuals and videos on [Dell | Support](#).

## Create device policy group in Wyse Management Suite

### About this task

You can create groups in Wyse Management Suite 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 a policy configuration has to be prioritized between the different levels, then the lowest-level policy takes precedence.

### Steps

1. On the **Groups & Configs** page, click the **Default Device Policy Group** option.
2. Click .
3. In the **Add New Group** dialog box, enter the **Group Name** and **Description**.
4. In the **Registration** tab, select the **Enabled** check box under **Group Token**.
5. Enter a group token.  
A group token is a unique identifier that is required to register the devices to a group.
6. 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 registration key
- Using legacy DNS record fields or DHCP scope options. See, [Registering devices by using legacy DHCP option tags](#) and [Registering devices by using legacy 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. The option is enabled by default. When enabled:

- Devices are displayed as **Pending Enrollment** within the **Devices** page.
- Administrators can then review and validate individual devices or select multiple devices for validation.
- After validation, the devices are assigned to the intended group.


For more information about how to validate the devices, see [Enrollment Validation](#).


# Register devices using Wyse Device Agent


## Prerequisites

Create a group in WMS and create a group token for the group. 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. Locate the Wyse Device Agent application icon  in the **System Tray** and open it. The **Wyse Device Agent** screen is displayed.
3. From the **Management Server** drop-down list, select **Wyse Management Suite**.
4. Enter the following server address and the port number in the respective fields.
  - **US data center**—us1.wysemanagementsuite.com/ccm-web
  - **EU data center**—eu1.wysemanagementsuite.com/ccm-web

 **NOTE:** If the server address contains **http**, a warning message is displayed. Click **Ok** to confirm.

5. Enter the group token.
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**.

# Dell Application Store

Dell Application Store is a software bundle consisting of Dell value-added applications.

Dell Technologies recommends that you install the following applications that are bundled in the Dell Application Store on the device:

- **Wyse Device Agent**—Wyse Device Agent (WDA) is a unified agent for device management solutions. If you install WDA, you can manage devices using Wyse Management Suite.
- **Wyse Easy Setup**—Wyse Easy Setup enables administrators to quickly and easily deploy configurations on devices. You can create a kiosk mode to lock down a Windows device to prevent users from accessing any features or functions on the device outside of the kiosk mode. You can customize the kiosk interface to control user access to specific features.
- **Dell Application Control Center**—Dell Application Control Center (DACC) DACC offers a user interface to manage device configurations, embedded applications, and utilities. It also provides a kiosk mode with centralized management capabilities.
  - **Application Launch Manager**—Application Launch Manager (ALM) enables you to start any application that is based on predefined events such as service startup, user logoff, or device shutdown in session zero. You can also configure multilevel logs which are essential for troubleshooting.
  - **xData Cleanup Manager**—xData Cleanup Manager (xDCM) keeps extraneous information from being stored on the local disk. xDCM can be used to automatically clean-up directories used for temporary caching of information. Clean-up is triggered on either service startup, user logoff, or device shutdown. It does the clean-up invisibly to the user and is configurable.
- **Dell Secure Client**—Dell Secure Client is a security software for Windows-based devices. This software protects your device by restricting unauthorized modifications to files, folders, and registry exclusions.
- **Overlay Optimizer**—Overlay Optimizer is a software component that works with Microsoft Unified Write Filter (UWF). Overlay Optimizer provides write protection and extends the uptime of devices. Overlay Optimizer monitors the UWF overlay space and the content. Overlay Optimizer identifies higher overlay space consumption in the write filter and moves the unused content to the Overlay Optimizer disk overlay. Clearing the UWF overlay extends the device uptime.

To deploy the package to the devices using WMS, see [Deploy an application or a package 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 repository** 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 installed components of Dell Application Store such as DACC, WDA, ALM, and so on, log in to Wyse Management Suite and go to **Devices > <Device Details page of the individual device> > Installed Apps**.



# WinIoT 2.x policy configurations in Wyse Management Suite

Wyse Management Suite 4.1 and later versions offers enhanced support for WinIoT 2.x policy configurations 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. 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, filter devices, and check the **OS Type** column.

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

## Prerequisites to enable WinIoT 2.x policy on the device

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

- Wyse Device Agent 14.6.9.x or later versions
- Wyse Easy Setup version 2.0.0.471 or later versions
- **Windows 10 IoT Config UI Enabler Package** with ConfigUISupport\_1.0.0.8.exe or later versions

**NOTE:** These components are included in WIE10 240x and later versions.

For the WMS cloud, you can deploy the ConfigUISupport\_1.0.0.8.exe or later version directly from the cloud.

For the WMS on-premises environment, you must download the latest **Windows 10 IoT Config UI Enabler Package** (ConfigUISupport\_1.0.0.8.exe or later versions) 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 or a package using WMS](#).

**NOTE:** If you are using Wyse Device Agent 14.6.8.x or earlier versions, 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. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **WinIoT 2.x**. The **Configuration Control | WinIoT 2.x** window is displayed.
3. Click **Advanced**.
4. 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

5. Configure the options as required.

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

6. 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 and remove them from 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.

**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 check box of the device or devices.
5. From the **More Actions** drop-down menu, click **Initiate UWF Servicing Mode**.


The screenshot shows the WMS 'Devices' page. At the top, there are various filter dropdowns for Configuration Groups, Status, OS Type (WinIoT 2.x), OS Subtype, DNS, Platform, Manufacturer, Agent Version, Subnet/Prefix, Timezone, Device Tag, OS Version, Ip Type, BIOS Version, Recovery Partition Status, and eMMC EOL Status. Below the filters is a table of devices. One device is selected, and the 'More Actions' menu is open, showing options like Factory Reset, Soft Reset, Rollback To Last Known Good Configuration, Change Group, Send Message, Clear User(s) Data, Start Ringing, Delete, Update WinIoT/ThinLinux image, Shutdown Now, Update Firmware, Update Firmware & Applications, Schedule Device Command, Schedule App Policy, Wake on LAN, and **Initiate UWF Servicing Mode** (highlighted with a red box). Other options include Tag device(s), unTag Device(s), Export All Devices to CSV, Convert to Dell Hybrid Clients, Bulk Change Group, Edit DeviceTag(s), and Reimage.

Name	Device Tag	Compliance	OS Type	Version	Serial#	IP Address	Last User	Group	Last Check-in	Health	Registered	Write Filter
[Selected]	N/A	[Red dot]	WinIoT 2.x	Windows 10	[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 Wyse Management Suite 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 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**.

# Deploy driver packages for Windows 10 IoT Enterprise LTSC 2021

You can deploy and install driver packages on devices running Windows 10 IoT Enterprise LTSC 2021 from Wyse Management Suite.

## 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](#).

# Deploy application or package using WMS

Dell Technologies recommends that you use the **Advanced App Policy** option if you want to deploy multiple applications to various subgroups. Also, **Advanced App Policy** option is available only in the Pro edition of WMS.

## Prerequisites

1. Copy and paste the application and the pre or post install scripts (if necessary) in the `thinClientApps` folder of the local repository or upload it directly to the WMS user interface. To upload directly to the WMS user interface, go to **Apps & Data > App Inventory > Thin Client** and click **Add WinIoT Package file**.
2. Go to **Apps & Data > App Inventory > Thin Client** and verify that the application is registered to WMS.

**NOTE:** The **App Inventory** interface takes approximately two minutes to populate any recently 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.

Apps & Data – Thin Client App Policies Local search

**App Inventory**

- Thin Client
- Wyse Software Thin Client
- Edge Gateway - Ubuntu Core
- Edge Gateway / Embedded PC
- Dell Hybrid Client
- Generic Client

**App Policies**

- Thin Client
- Wyse Software Thin Client
- Edge Gateway - Ubuntu Core
- Edge Gateway / Embedded PC
- Dell Hybrid Client
- Generic Client

### Add Advanced App Policy

Policy Name

Group  + ?  
 Default Device Policy Group

Sub Groups  Include All Subgroups

Task

OS Type   Filter files based on extensions ? ?

Application   +

Enable app dependency ?

OS Subtype Filter

Platform Filter

Apply Policy Automatically  ?

**Figure 2. Advanced App Policy**

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** check box 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**.

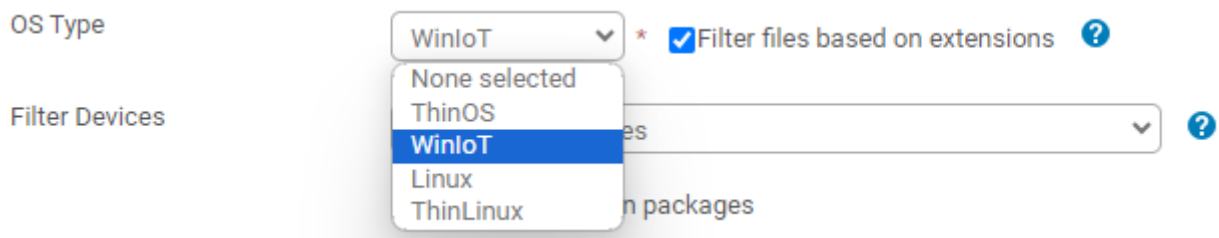


Figure 3. OS Type

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:

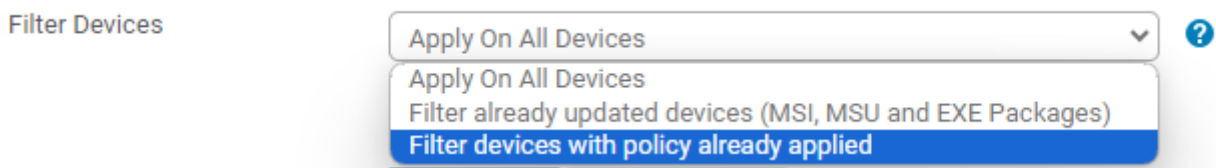


Figure 4. Filter devices

- 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**.

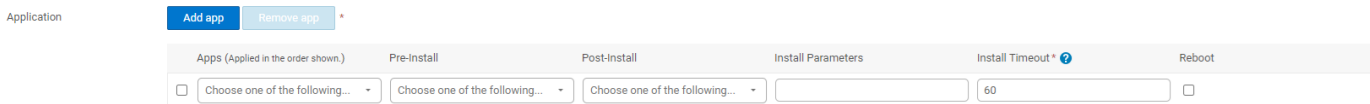


Figure 5. Add an application

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 Technologies supported third-party applications and their respective silent installation parameters:

Table 1. Third-party applications

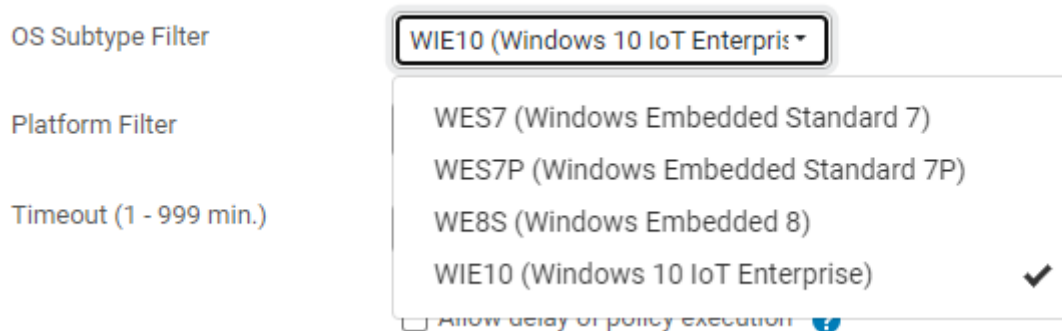
Application name	Silent installation parameters
Dell Application Store	--silent (If the WDA version lower than 14.6.9.23.) <b>NOTE:</b> The parameter is optional if the WDA version is 14.6.9.23 and higher.
VMware Horizon Client	--silent
Citrix Workspace app	--silent
Amazon WorkSpaces	--silent
Cisco Jabber Softphone for VDI (Virtual Desktop Infrastructure) Client	/qn
Cisco Webex App VDI Plugin (Bundled Webex Meetings VDI plugin)	/qn



**Table 1. Third-party applications (continued)**

Application name	Silent installation parameters
Zoom VDI Universal plugin	/quiet /norestart

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. To stop the application policy at first failure, select **Enable app dependency**.
15. From the **OS Subtype Filter** select **WIE10 (Windows 10 IoT Enterprise)**.



**Figure 6. OS Subtype Filter**

16. From the **Platform Filter**, select the device 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 implementation of the policy, 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.

**NOTE:** The job status of the newly added device count that is checked in to WMS is not displayed.

20. Select the **Skip write filter check** check box to skip the write filter cycles.  
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.
23. Select any of the following options:
  - **Immediately**—Server runs the job immediately.
  - **On device time zone**—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**—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.

# Schedule application policy

## Steps

1. On the **Jobs** page, click the **Schedule Application Policy** option.  
The **App Policy Job** screen is displayed.
2. From the drop-down list, select the application policy that you want to schedule.
3. Enter the job description.
4. From the **Run** drop-down list, select any of the following options:
  - **Immediately**
  - **On selected time zone and date/time**
  - **On selected date/time**
5. 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.
6. Select the time zone if you have selected **On selected time zone and date/time** in Step 4.
7. 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.
8. Click the **Preview** option to view the details of the scheduled job.
9. On the next page, click the **Schedule** option to initiate the job.

## 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.

## Add Package X

Choose a file to upload:

**Name**

\*

**Notes**

\*

Override existing file

**Select file repository for direct upload to Repository**

Nothing selected ▼

---

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 7. 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.