

# Windows 11 IoT Enterprise LTSC 2024

## Administrator's 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.....</b>	<b>6</b>
Document purpose.....	6
<b>Chapter 2: Getting started with Windows 11 IoT Enterprise LTSC 2024 .....</b>	<b>7</b>
Upgrading to Windows 11 IoT Enterprise LTSC 2024.....	7
Minimum hardware requirement.....	7
Logging in to the device.....	7
Before configuring your device.....	8
<b>Chapter 3: Dell Application Store.....</b>	<b>9</b>
<b>Chapter 4: Using Wyse Management Suite.....</b>	<b>10</b>
Wyse Management Suite versions.....	10
Create device policy group in Wyse Management Suite.....	10
Register devices to Wyse Management Suite.....	10
Register devices using Wyse Device Agent .....	11
WinIoT 2.x policy in Wyse Management Suite.....	11
Edit the WinIoT 2.x policy settings in WMS.....	11
Import Wyse Easy Setup configurations to WMS.....	12
Deploying applications using WMS.....	13
Schedule an application policy.....	15
Customizable WDA lock screen.....	16
Configure region and language settings from WMS.....	17
Install certificates using WMS.....	18
Configure password settings from WMS.....	19
Configure Broker agent connections from WMS.....	19
Add an application in Wyse Easy Setup using WMS.....	19
Configure Wyse Easy Setup from WMS.....	20
Configure domain settings from WMS.....	21
Configure BIOS settings and password using WMS.....	21
Sync BIOS admin password for WinIoT 2.x devices using WMS.....	22
Remotely shadow your client.....	22
Initiate remote shadow (VNC) connection using WMS.....	22
Initiate remote shadow (P2P) connection using WMS.....	24
Imaging Windows 11 IoT Enterprise LTSC 2024 devices using WMS.....	27
Capture image using WMS.....	27
Deploy an image using WMS.....	28
Upgrade BIOS using WMS.....	29
<b>Chapter 5: Local available applications.....</b>	<b>30</b>
Wyse Easy Setup.....	30
Configuring profiles.....	30
Import or export configurations.....	32
Configure connections and applications.....	32

User settings.....	33
User Interface settings.....	36
<b>Chapter 6: Local administrative features and utilities.....</b>	<b>38</b>
Add additional languages to Windows 11 IoT Enterprise LTSC 2024 operating system.....	38
Supported languages.....	39
Removing language and feature on-demand packages.....	39
Format any existing partition.....	41
Using custom fields.....	41
Hotkey Filter.....	41
Configure the Hotkey Filter.....	41
Unified Write Filter.....	42
Using Unified Write Filter.....	42
Configure Write Filter dashboard.....	42
Configure file or folder exclusion list of UWF.....	43
Configure registry exclusion list of UWF.....	43
Windows Updates with UWF Servicing Mode.....	43
Initiate UWF Servicing Mode manually from WMS.....	44
Run UWF Servicing Mode manually from the device.....	45
Run UWF Servicing Mode using a scheduled task.....	45
Application Launch Manager.....	46
Configure Application Launch Manager.....	46
xData Cleanup Manager.....	47
Configure xData Cleanup Manager.....	47
<b>Chapter 7: Remote system administration.....</b>	<b>49</b>
TightVNC—Server and Viewer.....	49
TightVNC—Pre-requisites.....	49
Using TightVNC Viewer to shadow a device.....	49
Configuring TightVNC server properties on the device .....	49
<b>Chapter 8: BIOS settings and upgrades.....</b>	<b>51</b>
Accessing BIOS settings.....	51
Unified Extensible Firmware Interface and secure boot.....	51
Upgrading BIOS.....	51
Upgrade BIOS using USB drive.....	51
<b>Chapter 9: Imaging Windows 11 IoT Enterprise LTSC 2024 devices.....</b>	<b>53</b>
Dell Imaging Manager.....	53
USB Imaging Prerequisites.....	53
Capture an image using USB.....	55
Deploy an image using USB.....	57
Bare Metal Recovery.....	58
<b>Chapter 10: Troubleshooting.....</b>	<b>60</b>
Capturing logfiles.....	60
Configuration of DebugLog XML file.....	60
Request a log file using WMS.....	60
View audit logs using WMS.....	61

Viewing events.....	61
Capture and locate the log files of an application.....	61
Viewing and exporting operating system image manifest files.....	62
View and export operating system image current manifest information .....	62
Error message while importing Wyse Easy Setup configurations from WMS.....	63
Keyboard customization issues.....	63
<b>Chapter 11: Frequently asked questions.....</b>	<b>64</b>
How to set up a smart card reader?.....	64
How to use USB Redirection? .....	64
How to add an application package to the WMS repository?.....	64
Can I configure Wyse Easy Setup locally on the device which is managed by WMS?.....	65
How do I import the local Wyse Easy Setup configurations to WMS?.....	66
Can I host operating system images in the WMS cloud repository?.....	66
<b>Chapter 12: End User License Agreement (EULA).....</b>	<b>67</b>
Dell End User License Agreement.....	67
Amazon WorkSpaces Application License Agreement.....	73
VMWARE END USER LICENSE AGREEMENT.....	77
LICENSE GRANT.....	77
Cisco General Terms.....	84
1. Scope and applicability.....	84
2. Use Rights.....	84
3. Free trials.....	85
4. End of life.....	85
5. Paying Your Approved Source.....	85
6. Confidentiality.....	85
7. Privacy and security.....	86
8. Ownership of intellectual property.....	86
9. Intellectual property indemnity.....	86
10. Performance standards.....	87
11. Liability.....	88
12. Termination.....	88
13. General provisions.....	88
14. Definitions.....	90
Important Links.....	92
Citrix Workspace End User License Agreement .....	93
Microsoft Software License Terms.....	101

# Introduction

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.

You can also install additional add-ons from the **Drivers and Downloads** page of the specific hardware platforms at [Dell | Support](#) to support a wide range of peripherals and features.

## Document purpose

This guide provides information and outlines detailed device configurations for administrators to manage and run devices running Windows 11 IoT Enterprise LTSC 2024. For more information about the new features specific to the operating system version, see *Windows 11 IoT Enterprise LTSC 2024 Release notes* at [Dell | Support](#).

# 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.

## Upgrading to Windows 11 IoT Enterprise LTSC 2024

Devices running Windows 10 IoT Enterprise LTSC 2021 can upgrade to Windows 11 IoT Enterprise LTSC 2024. To activate Windows 11 IoT Enterprise LTSC 2024 after the upgrade, you need a Product Key Entry Activation (PKEA) license key from Dell.

PKEA keys are unique 5x5 keys that can be obtained through [Dell.com](https://www.dell.com).

For more information, see the Windows 11 IoT Enterprise LTSC 2024 Upgrade Guide at [Dell | Support](https://www.dell.com/support).

**NOTE:** You must use WMS 5.0 and later versions with a Pro license to upgrade a group of devices remotely from Windows 10 IoT Enterprise LTSC 2021 to Windows 11 IoT Enterprise LTSC 2024.

WMS Standard does not support remote upgrades. Use a USB drive to locally upgrade a device from Windows 10 IoT Enterprise LTSC 2021 to Windows 11 IoT Enterprise LTSC 2024.

## Minimum hardware requirement

- Ensure the system includes at least 8 GB of RAM and a minimum of 128 GB of non-eMMC storage.

## 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, see [Unified Write Filter](#).


 **NOTE:** Use the information in this section when configuring the device locally. For remote configuration, WMS automatically handles Unified Write Filter (UWF).



# Dell Application Store

Dell Application Store comes with following Dell value-added applications:

## Wyse Device Agent (WDA)

Description—Enables you to quickly and easily deploy configurations on devices. To register a device using **Wyse Device Agent (WDA)** , see [Register devices using Wyse Device Agent](#).

Benefits—Allows you to manage devices using WMS.

## Wyse Easy Setup

Description—Enables you to quickly and easily deploy configurations on devices. To deploy **Wyse Easy Setup** configurations remotely, see [Configure Wyse Easy Setup from WMS](#). To use **Wyse Easy Setup** locally on the device, see [Wyse Easy Setup](#).


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. To locally manage **Application Launch Manager (ALM)** configurations on a device, see [Application Launch Manager](#).
  - 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. To locally manage Extra Data Cleanup Manager (xDCM) configurations on a device, see [xData Cleanup Manager](#).
  - 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**.

# 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, enabling administrators to manage the automatic or manual addition of devices 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.wysemagementsuite.com
    - **EU data center**—eu1.wysemagementsuite.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.

## WinIoT 2.x policy in Wyse Management Suite



By default, Windows 11 IoT Enterprise LTSC 2024 devices are managed by the WinIoT 2.x policy.

### Edit the WinIoT 2.x policy settings in WMS

Editing the WinIoT 2.x policy settings in WMS allows you to tailor the policy configurations to your specific needs and requirements.

### 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.  
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:** If needed, click the **Reset Policy** option to reset the policy to default configurations. Alternatively, click the **Reset Entire Policy** option to clear all configurations.
7. Click **Save & Publish** to save the changes and apply the updated policy configurations.  
 **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.


## Import Wyse Easy Setup configurations to WMS

As an IT administrator you can export the local Wyse Easy Setup configuration of a device into a JSON file. Using WMS, you can import the JSON file to remotely deploy configurations to other devices.

### Prerequisites

You must export a JSON file with Wyse Easy Setup configurations to the local device. For more information, see [Import or export configurations](#).

### Steps

1. Log in to WMS as an administrator.
2. On the **Groups & Configs** page, select your preferred group.
3. Click **Edit Policies** and select **WinIoT 2.x**.
4. Click **Import**.  
The **Import Policies Wizard** screen is displayed.
5. Select the **From an export file** mode.
6. Click **Browse** and select the JSON file containing the Wyse Easy Setup configurations.
7. Click **Next**.  
A preview of the policies in the selected group is displayed.
8. Click **Next**.  
The summary of the import process is displayed.
9. Click **Import**.  
 **NOTE:**
  - When you import a policy from a file, if there are references or invalid dependencies, the import fails and an error message is displayed. If the file to be imported has a reference or dependency file, go to the Edit Policy page of the respective device type and import the group policies.
  - If the destination group contains existing policies for the same device type, the newly imported policies replace them.

# 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

Before deploying applications, ensure the following:

The application and any required pre or post-install scripts are uploaded 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 **Apply On All Devices** for applying the policy to all devices.
  - Select **Filter already updated devices** for stopping redeployment of applications deployed through WMS.
  - Select **Filter devices with policy already applied** for excluding devices with the policy.
10. Click **Add app**.

From the **Apps (applied in the order shown.)** drop-down list, select an application. Optionally, add **Pre-Install**, **Post-Install** scripts, 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. Set an **Install Timeout** (default: 60 minutes).
12. Select **Reboot** if the device should restart after installation.



**NOTE:** It is mandatory to select **Reboot** 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.

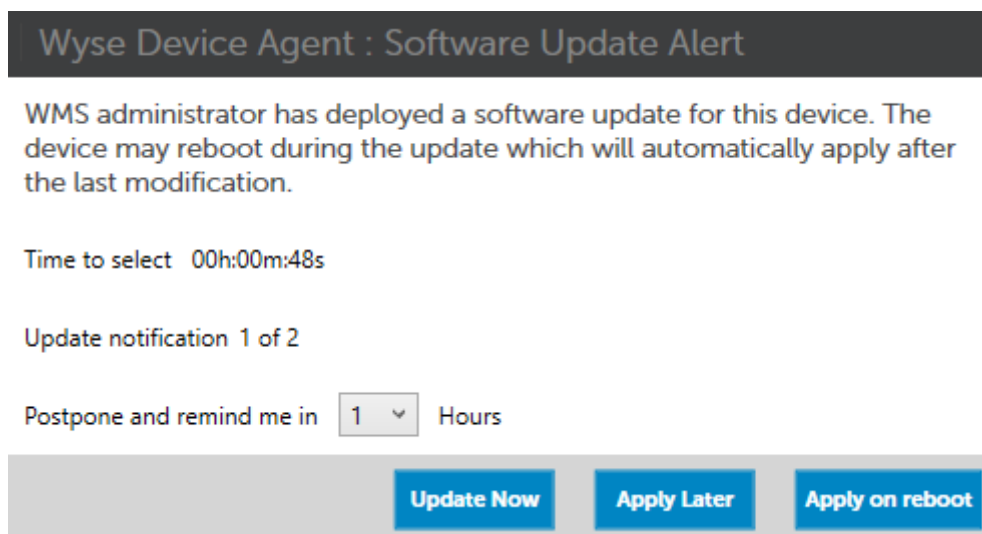
13. Click **Add app** again to include multiple applications.
14. **Enable app dependency** to stop the application policy if an application fails.
15. Select OS and platform filters: From the **OS Subtype Filter**, select **WIE11 (Windows 11 IoT Enterprise LTSC 2024)**.
  - **OS Subtype Filter:** Select **WIE11 (Windows 11 IoT Enterprise LTSC 2024)**.
  - **Platform Filter:** Choose the device model for deployment.
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 1. 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, choose one of the following options:
  - **Immediately**—Deploys the policy right away.
  - **On selected time zone and date/time**—Deploys based on a specific time zone.
  - **On selected date/time (of device time zone)**—Deploys according to the device local time.

6. Select **Exclude Offline Devices** to skip devices that are currently offline. Offline devices can be updated later from the Jobs page.  
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**.
8. Configure scheduling details:
  - **Effective**—Set the start and end date.
  - **Start between**—Define a time range for deployment.
  - **On day(s)**—Select specific days of the week.
9. Click **Preview** to review the details of the scheduled job.
10. Click **Schedule** to confirm and initiate the job.

## Customizable WDA lock screen

IT administrators configure the WDA lock screen using WinIoT 2.x Policy and Application Policy (Standard and Advanced). This configuration incorporates corporate branding elements and status indicators.

### Prerequisites

The customizable WDA lock screen feature needs the following requirements:

- Dell Application Store version 25.05.0.5 or later.
- Wyse Device Agent version 14.7.0.6 or later.
- Wyse Management Suite version 5.2 or later.
- Wyse Easy Setup version 2.0.0.664 or later.

### About this task

Customizing the WDA lock screen enhances the user experience by:

- Displaying corporate branding through custom logos.
- Showing operational status by indeterminate progress indicators.
- Providing contextual instructions through customized messages.

### Steps

1. Log in to WMS as an administrator.
2. Access policy configuration—
  - a. Go to the **Groups & Configs** page and select the target group.
  - b. From the **Edit Policies** drop-down menu, select **WinIoT 2.x**.  
The **Configuration Control | WinIoT 2.x** window is displayed.
3. Configure lock screen elements through WMS—
  - a. Go to **Advanced > WMS Settings > WDA Lock Screen Settings**.
  - b. Upload company logo (175 px recommended).  
Set the **WDA Lock Screen Logo** to display your company logo for branding.
  - c. Enter alert message for lock screen display.  
Configure the **Alert Message** to be shown on the lock screen.
4. Implement app policy customization using one of the following methods—
  - a. Standard Policy:
    - i. Go to **Apps & Data > App Policies > Thin Client**.
    - ii. Click **Add Policy**.
      - Complete all fields in the policy with the necessary information.
    - iii. Select **WinIoT** as **OS Type**.
    - iv. Check **Enable Custom Message**.
    - v. Enter **Custom Message Title** and **Custom Message**.
  - b. Advanced Policy:
    - i. Go to **Apps & Data > App Policies > Thin Client**.
    - ii. Click **Add Advanced Policy**.



- Complete all fields in the policy with the necessary information.
- iii. Select **WinIoT** as **OS Type**.
  - iv. Check **Enable Custom Message**.
  - v. Enter **Custom Message Title** and **Custom Message**.

## Results

After deploying these configurations, the customized WDA lock screen activates and shows:

- Corporate logo in header position.
- Indeterminate progress bar during operations.
- Custom alert messages if configured.

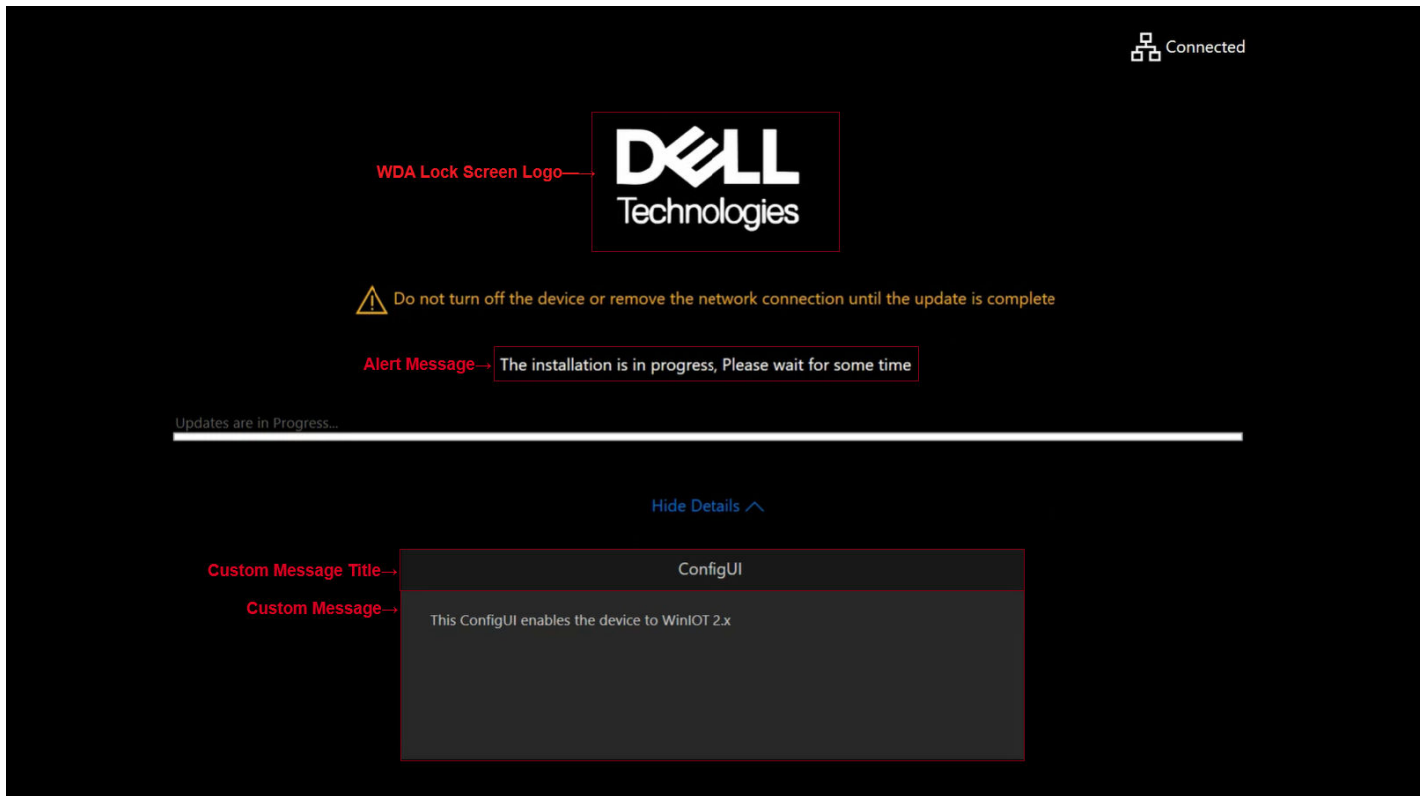


Figure 2. Customizable WDA lock screen

# Configure region and language settings from WMS

Configure region and language settings in WMS for specific groups and policies.

## 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. Click **Region & Language** and select any of the following options:
  - **Time Zone & Clock**—Configure the **Time Zone Setting** and **Clock Setting**.
  - **Language Setting**—Configure the **Display Language** and **Keyboard Layout** language options.
6. Click **Save & Publish**.

# Install certificates using WMS

You can upload and deploy multiple certificates to multiple Store Accounts and profiles. You can also assign different Store Type for a single certificate.

## 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. Click **Privacy & Security > Certificate**.
6. Choose from the following options:
  - **Install Certificates**—Deploy multiple certificates to a single Store Account and Certificate Store Type.
  - **Install Multiple Certificates**—Deploy a certificate to multiple Store Accounts and Certificate Store Types. Click **Add Row** for additional certificates.

Certificate

Install Multiple Certificates ☒ ⓘ ↻

Multiple Certificates		Add Row
Multiple Certificates 1 ⓘ		
Certificate Parameters		
Certificates	<input type="text" value="Select Certificate to Upload"/> <input type="button" value="Browse..."/> ⓘ	
Store Account	<input type="text" value="Select"/> ⓘ	
Certificate store type	<input type="text" value="Select"/> ⓘ	

Figure 3. Multiple certificates

### NOTE:

- If you have configured and deployed the settings using the **Install Certificates** option, you must reset the policy using **Reset Policy** before using the **Install Multiple Certificates** option.
- Uploading a Trusted Root Certificate to a Current User store account results in a security notification. This notification is displayed because the Trusted Root Store is secure, and deploying the certificate to a local system can prevent potential security issues.
- You can only add one certificate for a Store Account when using the **Install Multiple Certificate** option.

7. In the **Certificates** field, click **Browse** and select the certificate that you want to install.  
From the **Certificates** drop-down menu, select the certificate.
8. From the **Store Account** drop-down menu, select the appropriate option:
  - **Current user**—This type of certificate store is local to a user account on the device and is located under the HKEY\_CURRENT\_USER registry root.
  - **Local Computer**—This type of certificate store is local to the device, global to all users on the device, and located under the HKEY\_LOCAL\_MACHINE root in the registry.
  - **Both**—Select this option for both Store Accounts.
9. From the **Certificate store type** drop-down menu, select any of the following options:
  - **Personal**—For user-specific certificates.
  - **Trusted root certification authorities**—For trusted root certificates.
  - **Intermediate certification authorities**—For intermediate certificates in the chain.
10. Click **Save & Publish**.

# Configure password settings from WMS

You can configure the administrator and user passwords of the devices from 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. Click **Privacy & Security > Password Settings**.
6. Enable any of the following options to configure the local administrator and user password as required:
  - **Change Local Admin Password**
  - **Change Local User Password**
7. Click **Save & Publish**.

# Configure Broker agent connections from WMS

You can configure the Citrix, VMware Horizon, Azure Virtual Desktop (AVD), and Microsoft Remote Desktop settings from 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. Click **Broker Settings** and select any of the following options:
  - **Citrix Settings**
  - **VMware Horizon Settings**
  - **Azure Virtual Desktop (AVD) Settings**
  - **Microsoft Remote Desktop Settings**
6. Configure the options as required.
7. Click **Save & Publish**.

 **NOTE:** If you are configuring the Microsoft Remote Desktop settings, you can add and configure multiple RDP connections.

# Add an application in Wyse Easy Setup using WMS

You can add remote desktop applications such as VMware, Citrix, Amazon WorkSpaces, and Remote Desktop Protocol, and local applications such as Notepad in Wyse Easy Setup using 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. Click **Easy Setup > Kiosk Mode**.
6. Enable the **Kiosk Mode** option to replace the default Windows desktop with the Wyse Easy Setup desktop.

7. Enable the **Kiosk Reboot** option to reboot the device when the Kiosk mode is enabled.
8. In the **Application** field, click **Add Row**.
9. Enter or configure the following options:

**Table 2. Configuring the application settings**

Option	Description
Application Name	Enter the name of the remote desktop application.
Application Path	Enter the full path of the executable file as seen on the specific device.
Auto Launch	Enable the option if you want the application to launch automatically when you log in to the device.
Maximized	Enable this option if you want to open the application in a maximized window when you log in to the device.
Application Arguments	Enter the application argument values that must be passed to an application when it is started.
Custom Icon	If you want to add a custom icon to the application, enter the full path of the custom icon as seen on the specific device.
Application Exit Action	From the drop-down list, select the option that you want to use when you exit the Kiosk mode: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Shutdown upon Exit</b>—Shut down the device when you exit the application or connection.</li> <li>• <b>Restart upon Exit</b>—Reboot the device when you exit the application or connection.</li> <li>• <b>Logout upon Exit</b>—Log off from the signed user when you exit the application or connection.</li> <li>• <b>Persistent upon Exit</b>—Automatically relaunch the application when you exit the application or connection.</li> </ul>
Application State Retry Count	Enter the number of times the application must try to reconnect to the server if the network is lost. The retry count value should be between 2–10.
Application State Retry Interval	Enter the number of seconds between two retry attempts to reconnect the application to the server. The retry interval value should be between 30–360 s.

10. In the **Personalization** field, browse and add the background and logo for the Kiosk mode if required.
11. Click **Save & Publish**.

## Configure Wyse Easy Setup from WMS

You can configure and deploy Wyse Easy Setup configurations from WMS.

### Steps


1. Log in to WMS as an administrator with **WF** disabled.
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. Click **Easy Setup** and select any of the following options:
  - **Access Control**
  - **Kiosk Mode**
6. Configure the options as required.
7. Click **Save & Publish**.

For more information about configuring Kiosk Mode and remote desktop application in Wyse Easy Setup from WMS, see [Add an application in Wyse Easy Setup using WMS](#).

The following table describes the user persistence settings that are applied when the device is managed using WMS.

**Table 3. Display, Network, mouse and keyboard settings**

User type	After you restart the device	After you log in to a new session
Administrator	Device settings that are configured using WMS are applied.	Device settings that are configured using WMS are applied.
User—Using Windows Explorer when Control Panel settings (display, Network, mouse, and keyboard) are disabled.	Device settings that are configured using WMS are applied.	Device settings that are configured using WMS are applied.
User—Using the Control Panel settings when display, Network, mouse, and keyboard are enabled.	User-specific settings are retained after you restart the device.	User-specific settings are retained from the previous session.

 **NOTE:** Only a single user persistence configuration file exists for each user and it is shared when the client is managed locally or using WMS. The contents in the file vary according to the configuration deployed.

## Configure domain settings from WMS

You can set up domain settings in WMS by logging in as an administrator

### 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. Click **Network Configuration > Domain Settings** and configure the following options:


**Table 4. Domain settings**

Option	Description
Domain or Workgroup	From the drop-down list, select <b>Domain</b> or <b>Workgroup</b> .
Domain or Workgroup Name	Enter the domain or workgroup name.
User Name	Enter the username of the account which has the <b>Add to Domain</b> privileges.
Password	Enter the password for the user account specified in the <b>User Name</b> field.
Account OU	Enter the location of the organization unit where the computer object should be created. You must add semicolons and quotes as required. For example, "OU=testOU; DC=domain; DC=Domain; DC=com".
Auto Login	Enable this option to automatically log in to the device.

## Configure BIOS settings and password using WMS

You can configure BIOS settings such as device integration, wireless connections, password, device management, and so on, for different platforms using WMS.

### About this task


 **NOTE:** Configure BIOS settings and password is a WMS Pro feature.

### 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. Click **BIOS settings**.
6. Select the platform from the **Platforms** list and click **X**.
7. Configure the options as required.
8. Click **Save & Publish**.

## Sync BIOS admin password for WinIoT 2.x devices using WMS

### About this task


 **NOTE:** Sync BIOS admin password is a WMS Pro feature.

### 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. Click **BIOS settings**.
6. Select the platform from the **Platforms** list and click **X**.
7. Go to **BIOS Admin Password > Enable Admin Password**.


 **NOTE:** For **OptiPlex AIO 7410** and **OptiPlex AIO 7420**, go to **Security > BIOS Admin Password**.

8. Enter the password.
9. Click **Save & Publish**.

 **NOTE:** Sync BIOS Admin password option must be used when the BIOS password settings are changed. For information about how to use the option from WMS, see [Sync BIOS admin password](#).

## Remotely shadow your client

Global and group administrators can initiate remote shadow sessions using **VNC** or **P2P** protocols in Wyse Management Suite (WMS).

 **NOTE:** Remote Shadow (P2P) is supported in both WMS Cloud and on-premises deployments, but only for WMS Pro licenses. Remote Shadow (VNC) is available solely in on-premises deployments and supports both WMS Standard and WMS Pro licenses.

## Initiate remote shadow (VNC) connection using WMS

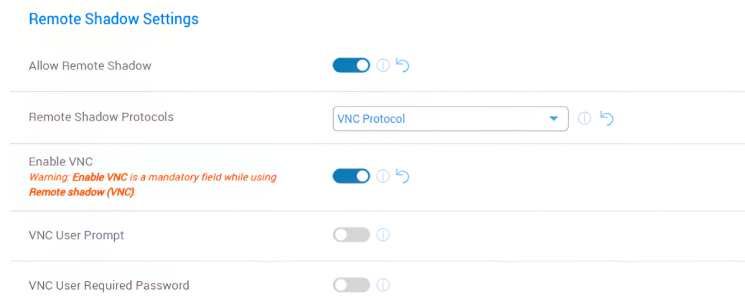
Global and group administrators can remotely access device sessions using WMS. This feature is available only in the private cloud version of WMS and supports both Standard and Pro licenses.

### About this task

Remote Shadow (VNC) requires configuration of **Remote Shadow Settings** in WinIoT 2.x policy followed by initiating the remote session using WMS.

## Steps

1. Log in to WMS as an administrator.
2. Configure the **Remote Shadow Settings** for VNC using WMS.
  - a. Go to the **Groups & Configs** page and select the target group.
  - b. From the **Edit Policies** drop-down menu, select **WinIoT 2.x**.
  - c. Go to **Advanced > WMS Settings > Remote Shadow Settings**.



**Figure 4. Remote Shadow Settings (VNC)**

The **Remote Shadow Settings** page is displayed.

- d. In the **Remote Shadow Settings** page, configure these parameters:
  - **Allow Remote Shadow**—Enable this option to select Remote Shadow (VNC).
  - **Remote Shadow Protocols**—Select VNC protocol.
  - **Enable VNC**—Enable this option to establish Remote Shadow (VNC), which is mandatory.
  - **VNC User Prompt**—Enable this option to display a notification on the client system, prompting the user to approve or reject the remote session.
  - **VNC User Required Password**—Enter the authentication password required for the administrator to initiate the Remote Shadow (VNC) connection.
- e. Click **Save & Publish**.
3. Initiate a Remote Shadow (VNC) Session Using WMS.
  - a. On the **Devices** page, select the device.  
The **Device Details** page is displayed.
  - b. From the **More Actions** drop-down list, select the **Remote shadow (VNC)** option.  
The IP address and the port number of the target device is displayed in the **Remote Shadow (VNC)** dialog box.  
**NOTE:** The default port number is 5900.
  - c. Optionally, change the port number of the target device.
  - d. Click **Connect**.  
**NOTE:** Wyse Management Suite portal supports a maximum of five remote shadow sessions per tenant.
  - e. Enter the password to initiate a remote session to the target device. The default password is: DELL.  
You can configure the password, port number, and other configurations. See, [Configuring TightVNC server properties on the device](#).

## Results

The end-user receives an Incoming TightVNC Connection dialog with **Accept** or **Reject** options.

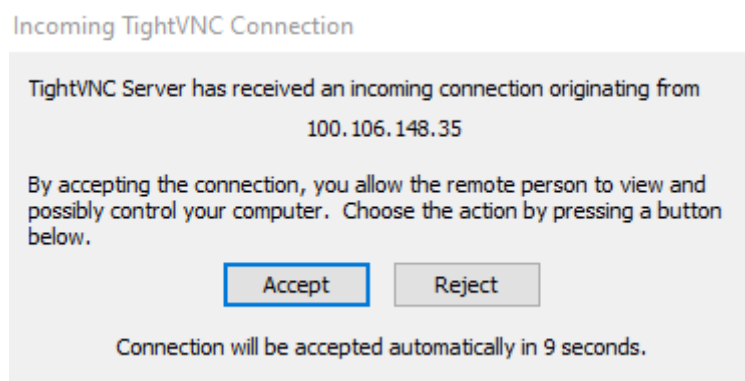


Figure 5. TightVNC Connection dialog

## Initiate remote shadow (P2P) connection using WMS

The Remote Shadow (P2P) feature enables WMS administrators to remotely view and interact with the logged-in user session of Windows 11 IoT Enterprise LTSC 2024. This capability allows efficient troubleshooting, guidance, and remote management directly through WMS. This chapter outlines the process to configure Wyse Management Suite (WMS) group settings for P2P Remote Shadow and initiate remote sessions. It includes enabling protocols, defining user consent policies, and establishing secure administrative access to endpoint devices.

### Prerequisites

The table below lists the features and limitations for Remote Shadow (P2P) connection using WMS:

Table 5. Features and Limitations of Remote Shadow (P2P) Connection Using WMS

Feature	Behavior	Limitations
Session Visibility	Only the active user session is accessible.	System-level sessions (such as Admin login) are not visible in User Mode.
Keyboard and Mouse Redirection	Admin inputs (keyboard/mouse) take priority within the WMS browser.	Local inputs (such as pressing the Windows key in WMS) trigger actions on the admin local system, not the client device.
Timeout Behavior	Performs the configured Accept or Reject action if no user response is received.	Sessions may autoapprove or deny based on the timeout policy (such as, 5 s).
View Only Mode	Restricts admin control to observation only (no keyboard/mouse input).	Admin interaction is disabled when this mode is enabled.

Ensure that the following requirements are met:

- Wyse Management Suite version 5.2 or later.
- Dell Application Store version 25.05.0.5 or later.
- Wyse Device Agent version 14.7.0.6 or later.

### About this task

Remote Shadow (P2P) requires configuration of **Remote Shadow Settings** in WinIoT 2.x policy followed by initiating the remote session using WMS.


### Important Notes:

- In Remote Shadow (P2P) sessions, some applications, and UI elements may be inaccessible or hidden. The restricted components include:
  - Accessibility tools such as **osk.exe**, **Narrator**, and **Voice Access**.
  - User Account Control (**UAC**) prompts.
  - Secure input windows.




For security reasons, the above-mentioned components run in isolated, secure desktop sessions that are separate from the default desktop. Microsoft Windows blocks screen capture and input redirection to the secure desktops to protect sensitive operations like password entry, system dialogs, and assistive technologies from being recorded or manipulated using normal applications, including Remote Shadow (P2P) screen capture.

- Before deploying any feature policies through Wyse Management Suite (WMS), install the Wyse Device Agent (WDA) on the target system.
- After a system restart or user sign-in, Microsoft Windows requires a physical mouse movement on the client device to display the mouse pointer during a Remote Shadow (P2P) session.


 **NOTE:** You can configure additional settings for remote shadow (P2P) connection using WMS. For more information, see [Additional configuration settings](#).

## Steps

1. Log in to WMS as an administrator.
2. Configure **Remote Shadow Settings** using WMS.
  - a. Go to the **Groups & Configs** page and select the target group.
  - b. From the **Edit Policies** drop-down menu, select **WinIoT 2.x**.
  - c. Go to **Advanced > WMS Settings > Remote Shadow Settings**.  
The **Remote Shadow Settings** page is displayed.
  - d. In the **Remote Shadow Settings** page, configure these parameters:
    - **Allow Remote Shadow:** Enable this option to activate Remote Shadow (P2P).
    - **Remote Shadow Protocols:** Select P2P protocol.
    - **Remote Shadow Password:** Enter the authentication password required for the administrator to initiate the Remote Shadow (P2P) connection.

 **NOTE:** Use a password with uppercase and lowercase letters, special characters, and numbers. Ensure that the password length is between 12 and 32 characters.

- **Enable Remote Shadow Prompt:** Enable this option to display a notification on the client system, prompting the user to approve or deny the remote session.
  - **Select Timeout Type:** Define the default action when the client device user does not respond to the prompt:
    - **Accept:** Automatically permit the remote session.
    - **Reject:** Automatically block the remote session.
  - **Timeout:** Specify the response window duration in seconds. Specify a value between **0 to 600 s**.
  - **Enable View Only:** Optionally, enable this option to restrict mouse and keyboard input during remote sessions, limiting the session to observation mode.
  - **Active Visible:** Enable this option to display real-time notifications to the user during the remote session.
- e. Click **Save & Publish**.  
The configuration is saved and assigned to the target devices.
3. Initiate a Remote Shadow session using WMS.
  - a. Select the target device. Go to **Devices > Device Details**.  
The **Device Details** window displays information that is related to the target device.
  - b. Go to **More Actions → Remote Shadow (P2P)** to start the remote session.
  - c. Enter the **Remote Shadow Password** configured in Step 1.

 **NOTE:** Initiate the Remote Shadow (P2P) session before initiating the Image Pull operation because Wyse Management Suite cannot communicate with the Wyse Device Agent during the Image Pull operation, which prevents Remote Shadow (P2P) from working.

The remote session is initiated. The end-user receives a Remote Access Request dialog with **Accept** or **Decline** options.

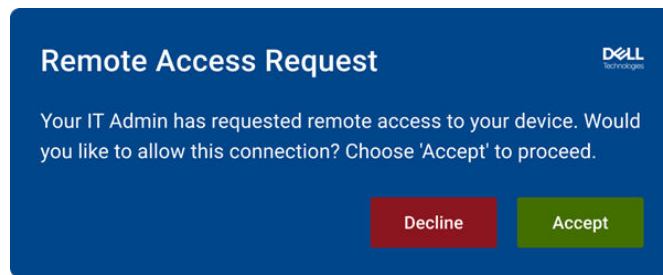


Figure 6. Remote access request on client system

## Results

When the end-user accepts, the administrator gains access to the session. If the user does not respond within the configured timeout, the session adheres to the **Accept** or **Reject** policy that is defined in the settings.

## Additional configuration settings

This section lists the additional configuration for Remote Shadow (P2P) settings in the WMS Portal Administration tab to manage remote shadow sessions.

### About this task

You can define various parameters for remote shadow sessions, such as the maximum number of concurrent connections and session timeouts, to optimize performance and security.

### Steps

1. Log in to WMS as an administrator.
2. Go to **Portal Administration > Console Settings > Other Settings**.  
The **Portal Administration — Other Settings** page is displayed.
3. In the **Portal Administration — Other Settings** page, go to **Remote Shadow (P2P) Configuration** section.

**Remote Shadow(P2P) Configuration**

Maximum Concurrent Remote Shadow Connections (1-30)	10
Idle Remote Shadow Session Timeout (1-20 minutes)	20
Maximum Remote Shadow Session Timeout (1-60 minutes)	20
No Connection Timeout (1-10 minutes)	10

Figure 7. Settings for remote shadow (P2P) configuration

4. Configure the following settings:
  - **Maximum Concurrent Remote Shadow Connections (1-30)** : This setting defines the maximum number of remote shadow sessions that can be active simultaneously. Administrators can set a value between 1 and 30 based on their requirements and network infrastructure capacity. For example, if set to 10, up to 10 remote shadow sessions can be active at the same time.
  - **Idle Remote Shadow Session Timeout (1-20 minutes)**: This setting specifies the duration of inactivity after which an idle remote shadow session automatically disconnects. The timeout can be set between 1 and 20 minutes. For example, if set to 5 minutes, the session disconnects if there is no activity for 5 minutes.
  - **Maximum Remote Shadow Session Timeout (1-60 minutes)**: This setting determines the maximum duration for a remote shadow session before it is automatically terminated. The timeout can be set between 1 and 60 minutes. [cite: 11] For example, if set to 30 minutes, the session will automatically end after 30 minutes, regardless of activity.

- **No Connection Timeout (1-10 minutes):** This setting defines the duration to wait for a connection to be established before timing out. [cite: 13] The timeout can be set between 1 and 10 minutes. For example, if set to 3 minutes, the system waits for 3 minutes to establish a connection before timing out.

## Results

When you complete these steps, the Remote Shadow (P2P) settings are configured according to your specifications, allowing for controlled management of remote shadow sessions.

# Imaging Windows 11 IoT Enterprise LTSC 2024 devices using WMS

This section details the Windows 11 IoT Enterprise LTSC 2024 operating system image capture and deployment process using Dell Imaging Manager and WMS.

## Capture image using WMS

### About this task

The following steps are applicable to capture a Windows 11 IoT Enterprise LTSC 2024 image using Wyse Management Suite.

**NOTE:** The **System Preparation Tool** generates an error during image capture. This error cancels the imaging process. This issue is specific to the Windows 11 Enterprise LTSC 2024 touchscreen devices and it is a Microsoft known issue.

Before reinitiating the imaging process, follow the steps below on the device to address this issue.

1. Log in to the device as an administrator, with the **Write Filter (WF)** disabled.
2. Using PowerShell, search for Handwriting packages: `(Get-AppxPackage -PackageTypeFilter Framework | ? {$_.PackageFullName -like "Microsoft.Ink*"}).PackageFullName`
3. Remove each package using the command: `Remove-AppxPackage -Package NAME-OF-PACKAGE`
4. Using PowerShell, search for the Handwriting.Main package: `(Get-AppxPackage -PackageTypeFilter Main | ? {$_.PackageFullName -like "Microsoft.Ink*"}).PackageFullName`
5. Remove the Handwriting.Main package using the command: `Remove-AppxPackage -Package NAME-OF-PACKAGE`
6. Search to confirm that all handwriting packages are removed (the output should return blank):  
`(Get-AppxPackage -PackageTypeFilter Framework | ? {$_.PackageFullName -like "Microsoft.Ink*"}).PackageFullName`

### Steps

1. Log in to WMS as an administrator.
2. Go to **Devices** and select your Windows 11 IoT Enterprise LTSC 2024 registered device.
3. Select **Pull OS Image** from the **More Actions** drop-down list.  
The **Pull OS Image** window is displayed.
4. Enter the **Name of image**, **File repository**, **Pull type**, and **Default options**.
5. Click **Prepare for Image Pull**.
6. Click **Pull Image**.  
The **Image Pull Request from System Admin** window is displayed on the registered device.
7. On the registered device, click **Pull after sysprep** to capture the image by running custom Sysprep.

- NOTE:**
- The device disables the **Write Filter (WF)** if it is enabled and prompts you to switch to the **Admin** account if not already in it. Ensure that the device is in the **Admin** account with the **WF** disabled.
  - Dell Technologies recommends using **Pull after sysprep** for image capture.

8. The **Create a new System Image** screen is displayed.

- Optionally, click the checkbox **Update Password** and enter a new password for both Admin and User profiles. The password must meet the complexity criteria set on the devices where the image is restored.

**NOTE:** When the **Update Password** is not selected, use the following default password credentials for the ISO image:

- Administrator account: Admin#<Service Tag of the device>
- User account: User#<Service Tag of the device>

Replace <Service Tag of the device> with the Service Tag for your device.

- Optionally, click the checkbox **Join a Domain** and enter the domain details to join the device to a specific domain postimaging process.
- Click **Capture Image**.
- The image capture process activates on the device, displaying progress indicators.

## Results

- After a successful capture, the device automatically logs in to the **User** account.
- Once the upload is successful and synced to WMS, the pulled image is displayed under **Apps & Data > OS Image Repository > WinIoT / ThinLinux** in WMS.

## Deploy an image using WMS

You can deploy an image to a device using WMS, but it is important to use only device-specific images. Images from other devices are not compatible.

### Steps

- Log in to the Wyse Management Suite (WMS) as an administrator.
- Go to **Apps & Data > OS Image Policies > WinIoT / ThinLinux**.
- Click **Add Policy**.  
The **Add WinIoT / ThinLinux Policy** screen is displayed.
- Enter a **Policy Name**.
- From the **Group** drop-down menu, select a group.
- From the **OS Type** drop-down menu, select **WinIoT**.
- From the **OS Subtype Filter** drop-down menu, select **WIE11 (Windows 11 IoT Enterprise LTSC 2024)**.
- From the **OS Image** drop-down menu, select the image file specific to the hardware platform. For more information, see *Add Windows Embedded Standard operating system and ThinLinux images to repository* in Dell Wyse Management Suite Version 5.0 Administrator Guide at [Dell | Support](#).
- From the **Platform Filter** drop-down menu, select the platform for which you want to deploy the image.
- From the **Rule** drop-down menu, select one of the following rules for the image policy:
  - Upgrade only.**
  - Allow downgrade.**
  - Force this version.**
- From the **Apply Policy Automatically** drop-down menu, select one of the following options:
  - Do not apply automatically:** The image policy is not applied automatically to a device registered with Wyse Management Suite.
  - Apply the policy to new devices:** The image policy is applied to a new device registered with Wyse Management Suite.
  - Apply the policy to devices on check-in:** The image policy is applied to a new device upon check-in that is registered with Wyse Management Suite.
- Click **Save**.
- An alert window is displayed.
- In the alert window, click one of the following options:
  - Later:** Schedule the policy later from the Jobs page.
  - Yes:** Schedule it immediately.


If you select **Yes**, the **Image Update Job** window is displayed.
- In the **Image Update Job** window, complete the following:
  - Enter the job description.

- b. From the **Run** drop-down list, select one of the following options:
  - **Immediately**: The server runs the job immediately.
  - **On selected time zone and date/time**: 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 date/time (of device time zone)**: The server creates one job to run at the date or time of the designated time zone.
- c. If you have selected **On selected time zone and date/time** in step 15(b), then from the **Time Zone** drop-down lists select the time zone.
- d. Enter or select the following options:
  - **Effective**: Select the days during which the policy should be deployed.
  - **Start between**: Select the time during which the policy should be deployed.
  - **On day(s)**: Select the days when the policy should be deployed.

16. Click **Preview**.


17. Click **Schedule**.

- On the device, a notification box appears indicating that the OS image download is in progress. The notification displays the image download progress.

 **NOTE:** When the same image is applied to the device again, the notification is not displayed.


- A notification bar is displayed to notify the user about the image application. Save ongoing work on applications before proceeding.
- Click **Ok** to start the imaging process immediately, or it begins automatically based on the scheduled wait time.
- Once the download has been completed, the deployment of the imaging process starts, and progress indicators display all critical tasks.


## Results

- The Windows 11 IoT Enterprise LTSC 2024 image is deployed successfully to the device.
  - In WMS, go to **Jobs** and check the details of the image job. The status shows **Success: 1**.
-  **NOTE:** The default password credentials for the Admin and User accounts in the Windows 11 IoT Enterprise LTSC 2024 ISO image are as follows:
- **Admin:** Admin#<Service Tag of the device>
  - **User:** User#<Service Tag of the device>

# Upgrade BIOS using WMS

## Steps

1. Go to [Dell | Support](#).
  2. Enter the **Service Tag** of your device, and click **Search**.
-  **NOTE:** If the **Service Tag** is not available, you can manually browse your device model.
3. Click **Drivers & Downloads**.
  4. From the **Operating system** drop-down menu, select **WIE11 (Windows 11 IoT Enterprise LTSC 2024)**.
  5. From the Category drop-down menu, select **BIOS**.
  6. Download the respective BIOS file.
  7. Deploy the file using the advanced application policy in WMS. For information about how to deploy the file, see [Deploy applications using WMS](#) and use the silent installation parameter `/s /p=<Password>`.

 **NOTE:**

- If the BIOS password is not changed, the default password is **Fireport**.

The lock screen is displayed during the package installation process on all the devices.

## Local available applications

VMware Horizon Client, Citrix WorkSpace App, and Microsoft Remote Desktop are preinstalled on the devices running Windows 11 IoT Enterprise LTSC 2024. You can also download the latest version of the applications from [Dell | Support](#). You can configure the Hotkey Filter to allow administrators to harden remote desktop sessions. Configuring the Hotkey Filter enables users to lock and unlock their remote desktop sessions without affecting the local Windows environment. For more information, see [Hotkey Filter](#).

**Table 6. Local available applications**

Local available applications	Product documentation
VMware Horizon Client	<a href="#">VMware Horizon Client Documentation</a>
Citrix WorkSpace App	<a href="#">Citrix Product Documentation</a>
Microsoft Remote Desktop	<a href="#">Microsoft Remote Desktop</a>

## Wyse Easy Setup

Wyse Easy Setup enables administrators to deploy configurations to devices.

Wyse Easy Setup enables you to:

- Create a dedicated browser-focused client by configuring the Internet Explorer and Microsoft Edge settings.
- Configure multiple Broker agent connections such as Citrix, VMware, and Microsoft RDP.
- Configure a device to create a dedicated application for a particular line of business.

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 also customize the kiosk interface to enable or disable user access to specific settings.

**NOTE:** As an administrator you must configure Wyse Easy Setup with **Write Filter (WF)** enabled. The device must be disconnected from the WMS server to enable configurations.

**WyseEasySetupAdmin** and **WyseEasySetupShell** can be located in the **Start** menu on the device. You can configure Wyse Easy Setup locally on the device or using WMS. For information about configuring Wyse Easy Setup using WMS, see [Configure Wyse Easy Setup from WMS](#).

## Configuring profiles

In Wyse Easy Setup, administrators can configure multiple profiles for different users and groups.

You can add multiple local users and local groups to a profile and deploy customized configurations to the profile. If a local user or a user domain is not added to a profile, they are added automatically to the default group.

You can add domain users and groups to a local group and deploy configurations.

The selected profile is displayed in the upper left corner, and the configurations of the selected profile are displayed in the administrator user interface.

**NOTE:**

- The default profile settings are applied to all users who are not added to a profile.
- If a local user or a domain user is added to multiple profiles, the settings that are configured for the first profile are applied.
- If a local user or a domain user is not added to any profile, they are added automatically to the default profile. The default profile is created automatically, and by default, all local users and groups are added to it.

## NOTE:


- The configurations that are deployed using Wyse Management Suite are deployed to the default profile and applied to all local and domain users. If the local configurations are applied to the same profile, then the configurations that are pushed through Wyse Management Suite are replaced by the local configurations. If the persistent user settings configurations for Mouse, Keyboard, Display, and WiFi are configured by a local user and also deployed using Wyse Management Suite, the local user configurations takes precedence.
- After the configurations are deployed to a profile, when a local user or domain user logs in to the administrator user interface, the configurations are reflected only if the profile is applicable to the logged-in user.


## Create a profile


### About this task


You can add multiple local users and local groups to a profile. You can also deploy customized configurations to the profile. This section describes the steps to create a profile and add users or groups to the profile.

### Steps

1. Go to **Start > Wyse > WyseEasySetupAdmin**.  
The Wyse Easy Setup user interface is displayed.
2. Click the **Profiles** tab.  
The **Profiles** window is displayed. By default, the **Default** profile is selected.
3. Click  to add a profile.
4. Enter the profile name and click the check mark next to the new profile name.


 **NOTE:** Profile names should be unique and should not contain more than 30 characters.

5. To add users or groups to the profile, select the check box in the **Users** and **Groups** window.
6. Click  in the **Change Profile** section.  
The new profile is added, and displayed on the Wyse Easy Setup administrator user interface.
7. Click **Apply**.

 **NOTE:** To save a new profile and the configurations, you must click **Apply** before closing the administrator user interface.



## Edit a profile

### About this task

 **NOTE:** You cannot edit the default profile.

You can edit the profile name and you can also add or remove local users and groups for a profile. This section describes the steps to edit a profile.

### Steps

1. Go to **Start > Wyse > WyseEasySetupAdmin**.  
The Wyse Easy Setup user interface is displayed.
2. Click the **Profiles** tab.  
The **Profiles** window is displayed.
3. Select the profile that you want to edit.
4. Click the  button in the **Profiles** tab.
5. Edit the profile name, and select or clear the check box in the **Users** and **Groups** window.
6. Click  in the **Change Profile** section.  
The profile is displayed on the Wyse Easy Setup administrator user interface.
7. Click **Apply**.



**NOTE:** All the configurations made to the current profile are lost when you select a different profile before you apply the changes.

## Preview a profile

### About this task

You can preview the settings configured to a profile by an administrator. This section provides information about the steps to preview a profile.

### Steps

1. Go to **Start > Wyse > WyseEasySetup shell**.
2. Select the profile from the **Profiles** drop-down list.  
The settings configured by an administrator are displayed.

## Delete a profile


### About this task



**NOTE:** You cannot delete the default profile.

You can delete a profile added to Wyse Easy Setup. This section describes the steps to delete a profile.


### Steps

1. Go to **Start > Wyse > WyseEasySetupAdmin**.  
The Wyse Easy Setup user interface is displayed.
2. Click the **Profiles** tab.  
The **Profiles** window is displayed.
3. Select the profile that you want to delete.
4. Click the  button in the **Profiles** tab.
5. Click **Yes**.  
The profile is deleted, and the first profile available in the **Profiles** tab is selected automatically.
6. Click **Apply**.




**NOTE:** You must click **Apply** (with default or any profile) to complete the deletion of the profile.

## Import or export configurations

- **Import Configuration**  —This option can import local configurations (JSON files), which can then be applied to the current machine by clicking **Apply**. The user must select the source folder and the file to import.



**NOTE:** Importing configurations to WMS is not supported.

- **Export Configuration**  —This mode can export current machine configurations to an external JSON file. The user can select the destination folder and filename for the output file. You can also export the configuration from a JSON file to WMS. For more information, see [Import Wyse Easy Setup Configurations to WMS](#).

## Configure connections and applications

### About this task

The **Connections & Applications** section in Wyse Easy Setup enables you to add and configure connections and applications for a user.



## Steps

1. Click the **+** icon in the **Connections & Applications** section.

The **Available applications/connections to add** dialog box is displayed.

The following options are available by default:

- RDP
- Citrix
- VMware Horizon View
- Browser
- Calculator
- Notepad
- Edge Browser

**NOTE:** To manually add an application, browse the application, and click **Import**.

2. Click the application or connection that you want to add and configure.

3. Click **Save**.

The configured application or connection is displayed in the **Connections & Applications** section.

4. Click **Apply**.

**NOTE:**

- You can add a maximum of 18 connections and applications in the Wyse Easy Setup shell.
- The device must be logged in using domain user credentials from the same domain as the server to connect to a Citrix VDI, VMware, or RDP environment using single sign-on.

## User settings

The **User Settings** section enables an IT administrator to configure the device-specific settings for users. This section contains the following options:

**Table 7. System**

Option	Description
Region/Language	Enable access to the region and language option in the control panel.
Date and Time	Enable access to the date and time option in the control panel.
Display	Enable access to the WyseEasySetup Display option in the control panel. When you enable this option, the device retains user-added configurations after rebooting. <b>NOTE:</b> If this option is configured using Wyse Management Suite, all the configurations are applied during the initial login. User changes made during a session take effect after the next login.
Network	Enable access to the <b>Network and Sharing Center</b> option in the control panel. When you enable this option, the device retains user-added configurations after rebooting. <b>NOTE:</b> If this option is configured using Wyse Management Suite, all the configurations are applied if the user logs in to the device for the first time. If the user changes these settings during a session, the new settings are applied when the user logs in to the device again.
Sound	Enable access to the sound option in the control panel.
Ease of Access	Enable access to the ease of access option in the control panel.

**Table 8. Peripherals**

Option	Description
Mouse	<p>Enable access to the mouse option in the control panel. When you enable this option, the device retains user-added configurations after rebooting.</p> <p><b>NOTE:</b> If this option is configured using Wyse Management Suite, all the configurations are applied if the user logs in to the device for the first time. If the user changes these settings during a session, the new settings are applied when the user logs in to the device again.</p>
Keyboard	<p>Enable access to the keyboard option in the control panel. When you enable this option, the device retains user-added configurations after rebooting.</p> <p><b>NOTE:</b> If this option is configured using Wyse Management Suite, all the configurations are applied if the user logs in to the device for the first time. If the user changes these settings during a session, the new settings are applied when the user logs in to the device again.</p>

## User persistence settings

Wyse Easy Setup supports user persistence settings. This feature enables you to automatically save your application settings from each session. The configured settings are applied during the next session.

The following tables describe the user persistence settings behavior when you restart or log off from the device.

**Table 9. Display and Network settings**

User type	After you restart the device	After you log in to a new session
Administrator	Default device settings are applied.	Display and Network settings from the previous session are preserved and applied in the current session.
User—Using Windows Explorer when Control Panel settings (Display and Network) are disabled.	Default device settings are applied.	Display and Network settings from the previous session are preserved and applied in the current session.
User—Using the Control Panel settings when Display and Network are enabled.	User-specific settings are retained after you restart the device.	User-specific settings are retained from the previous session.

**Table 10. Mouse and keyboard settings**

User type	After you restart the device	After you log in to a new session
Administrator	Default device settings are applied.	Mouse and keyboard settings from the previous session are preserved and applied in the current session.
User—Using Windows Explorer when Control Panel settings (mouse and keyboard) are disabled.	Default device settings are applied.	Mouse and keyboard settings from the previous session are preserved and applied in the current session.
User—Using the Control Panel settings when mouse and keyboard are enabled.	User-specific settings are retained after you restart the device.	User-specific settings are retained from the previous session.

The following table describes the user persistence settings that are applied when the device is managed using WMS.

**Table 11. Display, Network, mouse and keyboard settings configured from WMS**

User type	After you restart the device	After you log in to a new session
Administrator	Device settings that are configured using WMS are applied.	Device settings that are configured using WMS are applied.
User—Using Windows Explorer when Control Panel settings (display, Network, mouse, and keyboard) are disabled.	Device settings that are configured using WMS are applied.	Device settings that are configured using WMS are applied.
User—Using the Control Panel settings when display, Network, mouse, and keyboard are enabled.	User-specific settings are retained after you restart the device.	User-specific settings are retained from the previous session.

**NOTE:**

- Only a single user persistence configuration file exists for each user, and is shared when the client is managed locally or using WMS. The contents in the file vary according to the configuration deployed.
- Persistent settings are supported only for login-required user scenarios. They are not available for auto-login configurations.

The following table lists the mouse, keyboard, and Network settings that are saved automatically from the previous session.

**Table 12. Persistent mouse, keyboard, and Network settings**

User settings	Persistent settings
Mouse	<ul style="list-style-type: none"> <li>• Switch primary and secondary buttons.</li> <li>• Double-click speed</li> <li>• Turn on Click Lock.</li> <li>• Click Lock Time</li> <li>• Find the mouse pointer.</li> <li>• Hide mouse pointer—Display the location of the pointer when you press the <b>Control</b> key.</li> <li>• Pointer trail length</li> <li>• Snap mouse pointer</li> <li>• Scroll lines—vertical</li> </ul>
Keyboard	<ul style="list-style-type: none"> <li>• Character repeat delay</li> <li>• Character repeat rate</li> <li>• Cursor blink rate</li> </ul>
Network	<p>Preconfigured connections by an administrator or the configurations deployed using WMS.</p> <p><b>NOTE:</b> Wyse Easy Setup enables the users to connect and disconnect Network that persists after you reboot the device.</p>

## Configure the user persistent settings

User settings such as display, network, keyboard, mouse, and debug logs can be stored across various user profiles using Wyse Easy Setup.

### About this task

This section describes the steps to configure persistent user settings for a user profile using Wyse Easy Setup.

### Steps

1. Go to **Start > Wyse > WyseEasySetupAdmin**.  
The **Wyse Easy Setup Admin** interface is displayed.
2. Select the user from the **Profiles**.  
The **Current Profile** shows the selected user.

3. Go to the **User Settings**.
4. Enable the **Display, Network, Mouse, Keyboard**, and **Enable DebugLog**.
5. Click **Apply**.
6. Log in to the device as a user.
7. Go to **Start > Control Panel**.  
The persistent user settings are displayed and available for configuration.

## User Interface settings

The **User Interface** section enables you to configure the taskbar and the **Start** menu. You can also personalize the background and the logo on the user shell. The **User Interface** section contains the following options:

**Table 13. Kiosk mode**

Option	Description
Perform Reboot.	The device reboots after you apply any Wyse Easy Setup configurations.
Display Kiosk Mode	<p>When the Kiosk mode is enabled, the Wyse Easy Setup shell becomes the primary interface, replacing the traditional Windows desktop and taskbar. Users cannot access these standard Windows elements. However, users can switch between the active application and the connection using Alt+Tab keys.</p> <p><b>NOTE:</b> If the Kiosk mode is disabled, only RDP, Citrix, and VMware Horizon View connections configurations are displayed on the Windows desktop.</p>
Exit Action—Application	<p>Using this feature, you can define actions to be performed when a user closes an application.</p> <p><b>NOTE:</b> The <b>Exit Action</b> is enabled only if <b>Display Kiosk Mode</b> is enabled, and a single application or connection is configured.</p>
Smart Card On Removal	<p>When a smart card is removed, you can define the actions to be performed using this feature.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>This option is enabled only if <b>Display Kiosk Mode</b> is enabled.</li> <li>When you configure the device to remain unlocked, and you remove the smart card, you are logged off from the client desktop.</li> </ul>
Retry Count(2-10)	<p>Specify the maximum number of automatic reconnections attempts for Remote Desktop Protocol (RDP) sessions if there are network interruptions.</p> <p><b>NOTE:</b> To configure this option, you must enable KIOSK mode and set up one RDP connection setting.</p>
Retry Interval(30-360)	<p>Specify the number of seconds between two retry attempts to reconnect the Remote Desktop Protocol to the server.</p> <p><b>NOTE:</b> To enable this option, you must configure KIOSK mode and set up one RDP connection setting.</p>


**Table 14. Personalization**

Option	Description
Background	It enables the user to set a customized background. To set a customized background, click <b>Change</b> , and select the required background.
Logo	It enables the user to add a customized logo instead of the default Dell logo. To set a customized logo in the background, click <b>Change</b> , and browse to the required logo on your local drive. If you do not want any logo, then select the image at <drive C>\Program Files\Wyse\WyseEasySetup\Help\Images\NoLogo.png.

**Table 15. Taskbar**

Option	Description
Date and Time	It enables the user to set the date and time option in the taskbar on the Wyse Easy Setup shell or custom desktop.
24 Hours Format	It displays the time in a 24-hour format.
Sound	It enables the user to set the sound parameters in the taskbar on the Wyse Easy Setup shell or custom desktop.
Network Status	It enables the user to view the network option in the taskbar on the Wyse Easy Setup shell or custom desktop.
Touch Keyboard	It enables the user to view the touch keyboard on the Wyse Easy Setup shell or custom desktop.
StartMenu	It enables the user to view the <b>Start</b> menu on the Wyse Easy Setup shell or custom desktop.
Taskbar	It enables the user to view the <b>Taskbar</b> menu on the Wyse Easy Setup shell or custom desktop.

**Table 16. Start Menu**

Option	Description
Admin Mode	It enables the user to access administrator mode on the Wyse Easy Setup shell or custom desktop.
Allow Shutdown	It enables the user to shut down the device on the Wyse Easy Setup shell or custom desktop.
Allow Restart	It enables the user to restart the device on the Wyse Easy Setup shell or custom desktop.
Allow Log Off	It enables the user to log off from the device on the Wyse Easy Setup shell or custom desktop.
Allow Help	It enables the user to access <b>Help</b> file from the <b>Start</b> menu on the Wyse Easy Setup shell or custom desktop. <div>  <b>NOTE:</b> The <b>Help</b> file can be opened only using Internet Explorer. </div>

# Local administrative features and utilities

## Add additional languages to Windows 11 IoT Enterprise LTSC 2024 operating system

### Steps

1. Log in to the device as an administrator.
  2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
  3. Log in as an administrator.
  4. Go to **Start > Settings > Time & Language > Language & region > Add a language**.  
The **Choose a language to install** window is displayed.
  5. Search and select the required language.
  6. Click **Next**.  
The **Install language features** window is displayed.  
The **Install language pack** option is selected by default. You can select additional optional features of the language pack.
  7. Select the **Set as my Windows display language** option.
  8. Click **Install**.
  9. In the **Preferred languages** section, select the added language and click **More Options**.
  10. Download all the language packs.
  11. Restart the device and log in as an administrator.
  12. Go to **Start > Settings > Time & Language > Language & region**.
  13. Select the required **Country or Region** from the drop-down list.
  14. Go to **Time & Language > Language & region > Administrative language settings**.
  15. In the **Administrative** tab, click **Change system locale**.
  16. From the **Current system locale** drop-down list, select the required language.  
The device restarts.
  17. Log in as an administrator.
  18. Go to **Time & Language > Language & region > Administrative language settings**.
  19. In the **Administrative** tab, click **Copy settings**.
  20. Select the **Welcome screen and system accounts** and **New user accounts** options and click **OK**.  
The device restarts.
  21. Log in as an administrator.
  22. Open **Windows PowerShell** and run the following commands:
    - `Get-AppxPackage -AllUsers "*LanguageExperience*" | Remove-AppxPackage`
    - `Get-AppxPackage -AllUsers "*LanguageExperience*"`
- NOTE:**
- Verify the installation of the required language packs after running the command in step 22. If the language packs are missing, download the required language packs again.
  - Verify that the downloaded language packs are configured following the system reboot and before running Sysprep.
23. Go to **C:\ > Windows > Setup > Tools** and double-click the `LanguageConfig.exe` file.  
**Language Config** window is displayed.
  24. Select the required language and click **Apply**.

The language configuration completion message is displayed.

25. Click **Reboot Now**.

The device restarts.

26. Log in as an administrator.

### Next steps

Run the Sysprep process to convert the required language, see [Capture an image using WMS](#) or, [Capture an image using USB](#).

## Supported languages

The following are the list of languages that are supported in Windows 11 IoT Enterprise LTSC 2024 operating system:


**Table 17. Supported languages**

Language	Abbreviation
English	en-US
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Danish	da-DK
Dutch	nl-NL
Finnish	fi-FI
French	fr-FR
French Canadian	fr-CA
German	de-DE
Italian	it-IT
Japanese	ja-JP
Korean	ko-KR
Norwegian	nb-NO
Portuguese Brazilian	pt-BR
Russian	ru-RU
Spanish	es-ES
Swedish	sv-SE

## Removing language and feature on-demand packages

### Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in as an administrator.
4. Open the command prompt with administrator privileges.
5. Run the following command: `dism /online /get-packages | find /I "Client-Language"`.
6. View the **Supported Languages** table to identify the languages installed.
7. After the language has been identified, locate all the associated packages with that language.
8. Run `dism /online /get-packages | find /I "<Language Abbreviation>"`.

 **NOTE:** To get the **Package Identity** Version, execute the following command: `dism /online /get-packages`

9. Run the following commands to remove all language feature packages:

```
dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-Speech-  
<Language Abbreviation>-Package~31bf3856ad364e35~amd64~~<Package Identity Version>" /  
norestart
```

```
dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-  
TextToSpeech-<Language Abbreviation>-Package~31bf3856ad364e35~amd64~~<Package Identity  
Version>" /norestart
```

```
dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-OCR-  
<Language Abbreviation>-Package~31bf3856ad364e35~amd64~~<Package Identity Version>" /  
norestart
```

```
dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-  
Handwriting-<Language Abbreviation>-Package~31bf3856ad364e35~amd64~~<Package Identity  
Version>" /norestart
```

```
dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-Basic-  
<Language Abbreviation>-Package~31bf3856ad364e35~amd64~~<Package Identity Version>" /  
norestart
```

 **NOTE:** Not all the languages include the **LanguageFeatures-Speech** package. If the selected language includes the **LanguageFeatures-Speech** package, then that package must be removed.

10. After the **LanguageFeature** packages are removed, remove the **Client-LanguagePack** using the command `start /b /wait dism /online /remove-package /packagename:"Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~<Language Abbreviation>~<Package Identity Version>" /norestart`.
11. Repeat the steps to remove all the unused languages from the device.
12. After removing the unused languages, reboot the device.
13. After the device reboots, log in as an administrator and run the `OSComponentCleanup` utility.
14. Enable **Unified Write Filter**.

### Next steps

- Double-byte character languages such as Chinese Simplified, Chinese Traditional, Japanese and Korean include the following **Feature On Demand** packages that must be removed, if the languages are removed from the device:

- Chinese Simplified

```
Microsoft-Windows-LanguageFeatures-Fonts-Hans-  
Package~31bf3856ad364e35~amd64~~<Package Identity Version>
```

- Chinese Traditional

```
Microsoft-Windows-LanguageFeatures-Fonts-Hant-  
Package~31bf3856ad364e35~amd64~~<Package Identity Version>
```

```
Microsoft-Windows-InternationalFeatures-Taiwan-  
Package~31bf3856ad364e35~amd64~~<Package Identity Version>
```

- Japanese

```
Microsoft-Windows-LanguageFeatures-Fonts-Jpan-  
Package~31bf3856ad364e35~amd64~~<Package Identity Version>
```

- Korean

```
Microsoft-Windows-LanguageFeatures-Fonts-Kore-  
Package~31bf3856ad364e35~amd64~~<Package Identity Version>
```

These packages are not dependent on any other packages, hence can be removed at any time.

- You must remove the **LanguageFeatures-Basic** package.



# Format any existing partition

You can format a partition or volume on a hard disk if you are logged in as an administrator and the Write Filter (**WF**) is disabled. For detailed instructions, refer to the section titled *To Format an Existing Partition (Volume)* in the [Disk Management in Windows](#) guide.

## Using custom fields

To enter the configuration strings for use by the WMS, use the **Custom Fields** dialog box. These strings can be used to identify devices based on location, user, administrator, contacts, room, floor, and other criteria. The custom fields information is published to the WMS server, enabling IT administrators to manage the device and differentiate it from other devices.

### About this task

To input information for use by the WMS server, follow these steps:

#### Steps

1. Log in as an administrator.
2. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.  
The **Application Control Center** window is displayed.
3. On the left navigation bar, go to **UTILITIES > Custom Fields**.
4. Enter the custom field information in the custom field boxes, and click **Apply**.  
The custom field information is transferred to the Windows registry which is then available to the WMS server.

## Hotkey Filter

Hotkey Filter is a configurable tool that allows administrators to harden remote desktop sessions. It enables users to lock and unlock their remote desktop sessions without affecting the local Windows environment. In many deployment scenarios, access to the local Windows desktop and file system is unnecessary and can pose a potential risk. By using the Hotkey Filter, administrators can ensure that local resources remain inaccessible during remote sessions which reinforce the overall security posture.

## Configure the Hotkey Filter

#### Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in as an administrator.
4. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.  
The **Application Control Center** window is displayed.
5. On the left navigation bar, go to **UTILITIES > Tools**.
6. In the **Hotkey Filter** section, select any of following keyboard combinations that must be disabled:
  - **Ctrl+Alt+Del**
  - **Windows+L**
  - **Shift+Ctrl+Esc**
7. If you want to allow only the administrators to use the Windows security key combinations, select the **Always allow administrators to use Windows security keys on this computer** option.
8. Click **Apply** and restart the device.

# Unified Write Filter

Unified Write Filter (UWF) is a sector-based Write Filter that is designed to protect your storage media. UWF redirects write attempts to a virtual overlay, intercepting writes to the protected volume. This enhances device stability and reliability while reducing wear on write media, such as solid state drives (SSDs).

 **NOTE:** In this document **Unified Write Filter (UWF)** is addressed as **Write Filter (WF)**.

In UWF, an overlay is a virtual storage space that captures changes that are made to the protected volume. When the file system attempts to modify a protected sector, UWF copies the sector to the overlay and updates it there. If an application reads from that sector, UWF returns the data from the overlay, making it appear as though the volume has been written to, while it remains unchanged.

Upon device startup, the UWF utility starts automatically. You can add specific files or folders on a protected volume to a file exclusion list, allowing them to bypass UWF filtering. Writes to these excluded files or folders are written directly to the protected volume and persist after a device restart.

For more information, see the [Unified Write Filter documentation](#).

## Using Unified Write Filter

### About this task

To configure devices using UWF, do the following:

#### Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Configure the device as per your requirements.
4. After you configure the device to enable the Unified Write Filter, double-click the **Dell Wyse WF Enable** icon on the desktop.  
This icon enables the filter, and the device restarts. Your configurations on the device are now saved, and they persist after you reboot the device.

## Configure Write Filter dashboard

#### Steps

1. Log in to the device as an administrator with **WF** disabled.
2. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.  
The **Application Control Center** window is displayed.
3. On the left navigation bar, go to **WRITE FILTER MANAGER > Write Filter Dashboard**.
4. In the **Write Filter Dashboard** section, do the following and click **Apply**:
  - **Write Filter Status**—Displays the status of the Write Filter. You can also enable or disable the Write Filter.
  - **Current Overlay Size**—Displays the space that is reserved for overlay.
  - **Warning Threshold**—Displays the UWF cache percentage value at which a Low Memory warning message is displayed to the user for the current session.
  - **Critical Threshold**—Displays the UWF cache percentage value at which a Critical Memory warning message is displayed to the user. Once the memory level crosses the warning level 2, the device automatically restarts.
  - **Amount of RAM used for UWF Cache**—Displays the amount of RAM allocated to the UWF cache for the current session in Megabytes (MB).
5. In the **Write Filter Settings** section, configure **Amount of RAM to be used for UWF Cache** and click **Apply**. You can configure the amount of RAM that is to be used as the UWF cache for the next session in MB. This value must be in the range of 1024 MB to 2560 MB. There is an extra check to ensure that this value does not exceed 50% of the total available RAM.
6. In the **Write Filter Threshold Settings** section, do the following and click **Apply**:

- **Warning Threshold**—Set the UWF cache percentage value at which a Low Memory warning message is displayed to the user for the current session. The default value is 80, the minimum value is 50, and the maximum value is 80.
- **Critical Threshold**—Set the UWF cache percentage value at which a Critical Memory warning message is displayed to the user. The default value is 90, the minimum value is 80, and the maximum value is 95.

## Configure file or folder exclusion list of UWF

You can add and remove a file or directory to or from the exclusion list of the Write Filter. The **Current Session** column lists the files or directories that are excluded from the Write Filter function in the current session. The **Next Session** column lists the files or directories that are excluded from the Write Filter function in the next session and the changes are not committed until an administrator restarts the device.

### Steps

1. Log in to the device as an administrator with **WF** disabled.
2. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**. The **Application Control Center** window is displayed.
3. On the left navigation bar, go to **WRITE FILTER MANAGER > Commits & Exclusions > File Manager**.  
You can view the file or folder that is excluded from the current and next session.
4. Click **+ Add** under the **Next Session** list to add the file or folder to be excluded from the next session.
5. Click **+ Add** under **Commit a File** list to exclude a file from the Write Filter function.
6. After you add the file, select the file from the **Commit a File** list and click **Commit**.  
The **Changes made to the files listed are committed** message is displayed.

### Next steps

To remove file or folder from the list, select the file or folder, and click **Delete**.

## Configure registry exclusion list of UWF

You can add and remove a Registry key path to or from the exclusion list of the Write Filter. The **Current Session** column lists the Registry key path that is excluded from the Write Filter function in the current session. The **Next Session** column lists the Registry key path that is excluded from the Write Filter function in the next session and the changes are not committed until an administrator restarts the device.

### Steps

1. Log in to the device as an administrator with **WF** disabled.
2. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**. The **Application Control Center** window is displayed.
3. On the left navigation bar, go to **WRITE FILTER MANAGER > Commits & Exclusions > Registry Manager**.  
You can view the file or folder that is excluded from the current and next session.
4. Enter the path of the registry in the **Registry Key Path** field under the **Next Session** list to add the registry to be excluded from the next session.
5. Click **+ Add**.
6. Enter the path of the registry in the **Registry Key Path** and the **Value Name** under **Commit a File** list to exclude it from the Write Filter function.
7. Click **+ Add**.
8. After you add the details, select the registry path from the **Commit Registry** list and click **Commit**.  
The **Changes made to the registry are committed** message is displayed.

## 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.

## 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**.

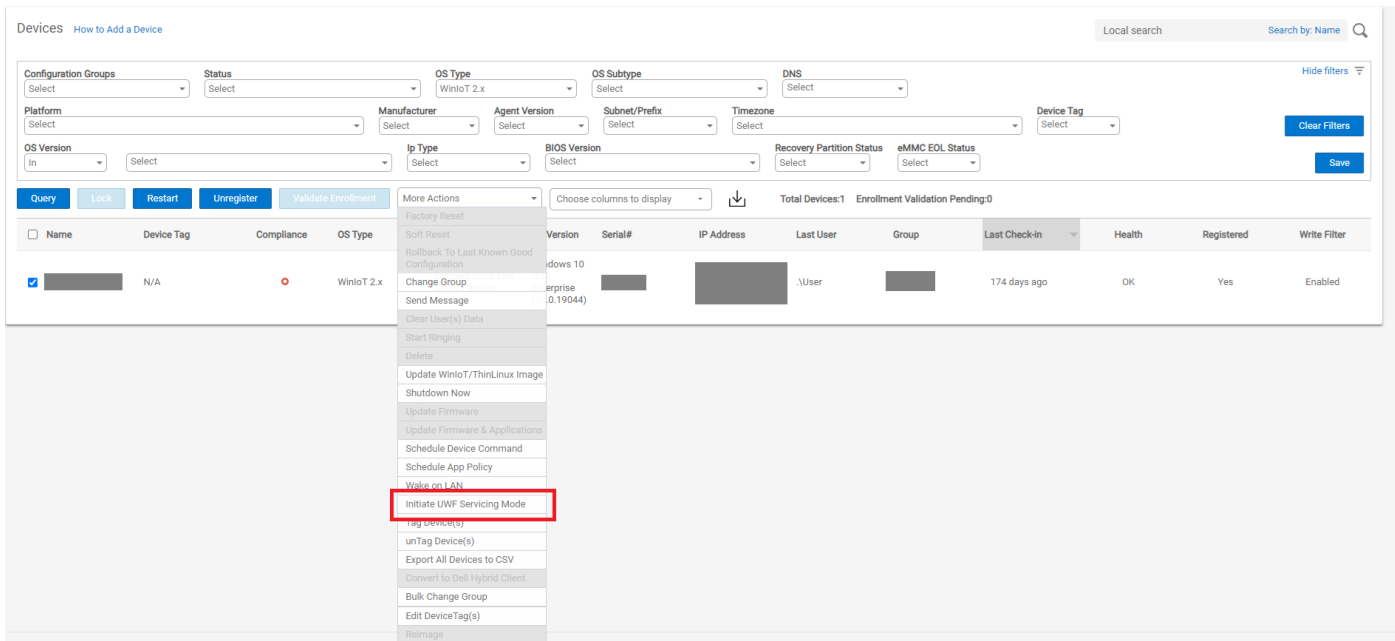


Figure 8. Initiate UWF Servicing Mode

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 (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.

## Run UWF Servicing Mode manually from the device

The UWF Servicing Mode can be triggered manually from the device.

### Steps

1. Log in to the device as an administrator.
2. Disable **Write Filter**.
3. Log in as an administrator.
4. Go to `C:\Windows\System32\oem`.
5. Run the `SystemServicing.bat` file as an administrator.

## Run UWF Servicing Mode using a scheduled task

You can enable the UWF Servicing Mode using a scheduled task on the devices. This option is disabled by default.

### Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in as an administrator.

4. Go to **Start > Task Scheduler**.
5. On the left pane, click **Task Schedule Library**.
6. On the right pane, right-click **WindowsUWFServicing** and select **Properties**.
7. Configure the options as required to run the UWF Servicing Mode.
8. Click **Ok**.
9. Right-click **WindowsUWFServicing** and click **Enable**.
10. Enable the **WF**.

## Application Launch Manager

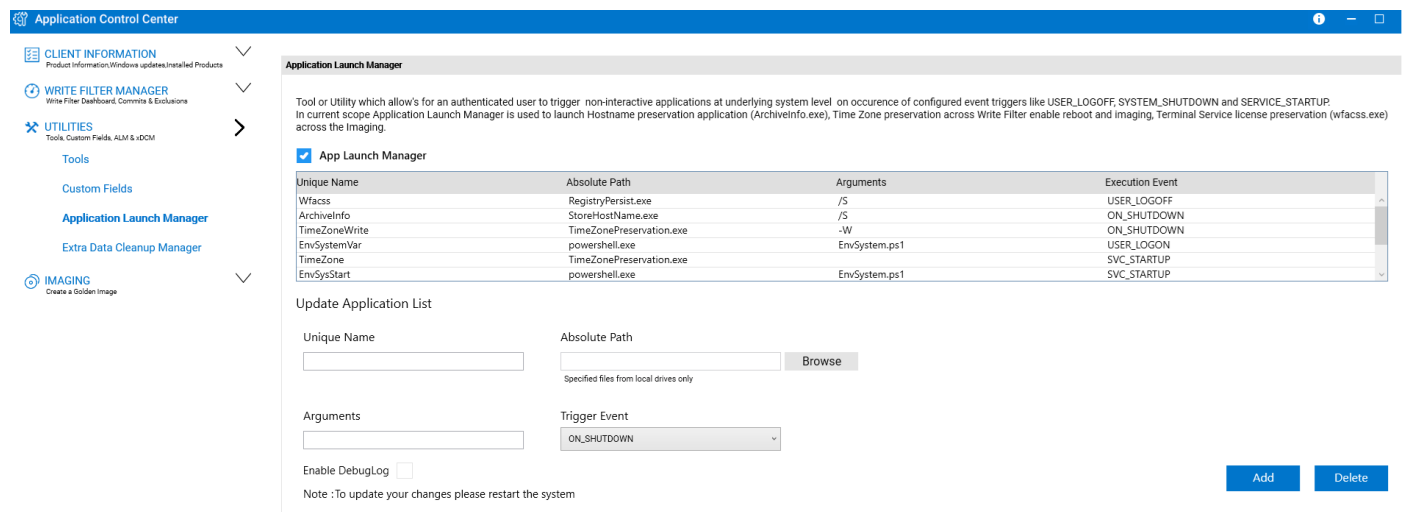
The Application Launch Manager (ALM) enables you to start an application that is based on predefined events such as service startup, user login/logoff, or system shutdown in system account.

## Configure Application Launch Manager

You can configure Application Launch Manager using the **Dell Application Control Center**. You can configure the applications to start when an event is triggered.

### Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in to the device as an administrator.
4. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.  
The **Application Control Center** window is displayed.
5. On the left navigation bar, go to **UTILITIES > Application Launch Manager**.  
You can view the applications details and the execution event.



**Figure 9. Application launch Manager**

6. In the **Update Application List** section, enter the following details:
  - **Unique Name**—Enter the name of the application.
  - **Absolute Path**—Browse to the location of the .exe file of the application.
  - **Arguments**—Optionally, enter any arguments for the application.
  - **Trigger Event**—From the drop-down list, select the event that triggers the application to start.
7. Click **Add**.

The application details are added to the list.

- Restart the system to update the changes.

### Next steps

To remove an application from the list, select the application, and click **Delete**.

## xData Cleanup Manager

xData Cleanup Manager (xDCM) prevents extraneous information from being stored on the local disk. xDCM can be used to automatically clean up directories used to temporarily cache the information. A clean up is triggered on either service startup, user logoff, or system shutdown.

## Configure xData Cleanup Manager

You can configure xData Cleanup Manager using the **Dell Application Control Center**. You can configure the xData Cleanup Manager to clean up the files or folders when an event is triggered.

### Steps

- Log in to the device as an administrator.
- Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
- Log in as an administrator.
- Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.  
The **Application Control Center** window is displayed.
- On the left navigation bar, go to **UTILITIES > Extra Data Cleanup Manager**.  
You can view the folder and file cleanup list.

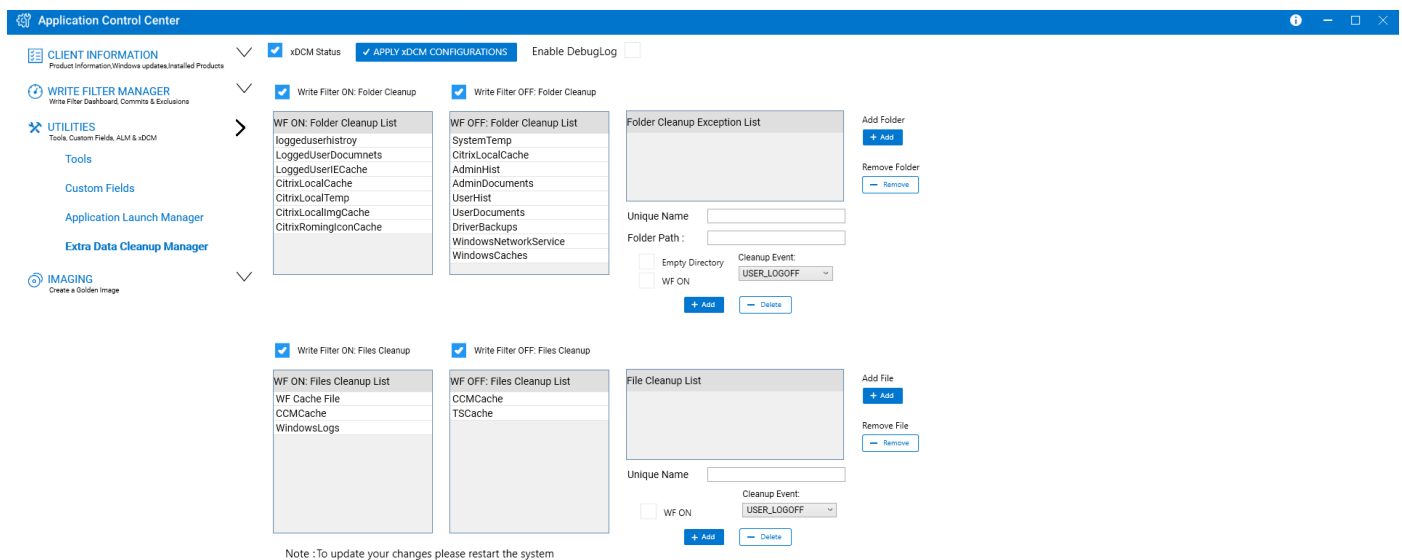


Figure 10. Extra Data Cleanup Manager

- To add the file or folder to the list, configure the following options and click **Add**:
  - Unique Name**—Enter the name of the folder or file.
  - Folder Path**—Browse to the location of the folder.
  - Empty Directory**—Select this option if you want to empty the directory of the folder.
  - WF ON**—Select this option if you want the event to be triggered when the Write Filter is enabled.
  - Cleanup Event**—From the drop-down list, select the option that triggers the cleanup.

Unique Name

Folder Path :

☐ Empty Directory

☐ WF ON

Cleanup Event:  
USER\_LOGOFF

+ Add    - Delete

**Figure 11. Add folder to xDCM**

7. Restart the device to update the changes.

**NOTE:** You can follow the same steps to clean up the files. You must add the **Unique Name**, select or clear the **WF ON** option, and select the **Cleanup Event**.

### Next steps

You can also add folders and files to the exception list to skip the cleanup of the selected folder or file.


1. Click **+ Add** under **Add Folder** or **Add File**.
2. Browse to the folder or file and click **OK**. The **Folder CleanUp Exception** or **File CleanUp Exception** window is displayed confirming the folder or file selection.
3. Click **Ok**.



# Remote system administration

## TightVNC—Server and Viewer

TightVNC is primarily intended for support and troubleshooting purposes.

 **NOTE:** TightVNC Server is preinstalled on the device.


You can download and install TightVNC Viewer from the TightVNC website. After installation, the Viewer can be used to shadow, operate, and monitor a device that runs Windows 11 IoT Enterprise LTSC 2024 operating system from a remote device.

TightVNC Server starts automatically as a service when the device restarts. The initialization of TightVNC Server can also be controlled by using the **Services** window.

## TightVNC—Pre-requisites

Before you install TightVNC Viewer on a remote machine, to access the device, you need the following:

- IP address or valid DNS name of the device to shadow, operate, or monitor. You can find the IP address by hovering over the TightVNC icon in the taskbar.
- Primary password of the device to shadow, operate, or monitor.

 **NOTE:** To establish a connection to a device that runs Windows 11 IoT Enterprise LTSC 2024 operating system using TightVNC, the default password is **DELL**.

## Using TightVNC Viewer to shadow a device

### Steps

1. Go to **Start > TightVNC**.
2. Open the **New Tight VNC Connection** dialog box.
3. Enter the IP address or valid DNS name of the device that is to be shadowed or operated or monitored.
4. Click **OK**.  
The **VNC Authentication** dialog box is displayed.
5. Enter the **Password** of the device that is to be shadowed.  
This password is the primary password of the device that is to be shadowed.
6. Click **OK**.  
The device that is to be shadowed or operated or monitored is displayed for the administrator in a separate window on the remote machine. Use the mouse and keyboard to operate the remote machine.

## Configuring TightVNC server properties on the device

TightVNC Server starts automatically as a service upon device startup. The TightVNC Server service can also be stopped and started by using the **Services** window.

### Steps

1. Log in to the device as an administrator with **WF** disabled.
2. To open the **TightVNC Server Configuration (offline)** dialog box, go to **Start > TightVNC > TightVNC Server — Offline Configuration**.  
The **TightVNC Server Configuration (offline)** window is displayed.

3. In the **Server** tab, set the **Primary password**. Use this password while shadowing the device.

The default primary password is **DELL**.

 **NOTE:** The maximum length of the password should be 8.

4. In the **Server** tab, select the following options:

- **Accept incoming connections**
- **Require VNC authentication**
- **Enable file transfers**
- **Hide desktop wallpaper**
- **Show icon in the notification area**
- **Serve Java Viewer to web clients**
- **Use mirror driver if available**
- **Use D3D driver if applicable**

5. Clear the following options:


- **Block remote input events**
- **Block remote input on local activity**
- **No local input during client sessions**
- **Connect to RDP session**

6. In the **Main server port** box, enter **5900**.

7. In the **web access port** box, enter **5800**.

8. In the **Screen polling cycle** box, enter **1000**.

9. Click **OK**.


 **NOTE:** For security purposes, Dell Technologies recommends that the primary password must be changed immediately upon receipt of the device and it is for administrator use only.

# BIOS settings and upgrades

To maintain your device environment, you can perform BIOS settings and upgrades locally using a USB drive or remotely from WMS.

## Accessing BIOS settings

### Steps

1. During the device start-up, press F2 when you see a Dell logo.  
The **BIOS Setup** screen is displayed.  
 **NOTE:** The default BIOS password is **Fireport**.
2. Change the BIOS settings as required.
3. Save the changes and exit.

## Unified Extensible Firmware Interface and secure boot

Unified Extensible Firmware Interface (UEFI) is a standard firmware interface that is designed to improve software interoperability and address limitations of BIOS. UEFI is designed to replace the Basic Input Output System (BIOS).

Secure Boot is a feature on UEFI-based clients that help increase the security of a client by preventing unauthorized software from running on a client during the boot sequence. It checks whether each software has a valid signature, including the operating system that is loaded during booting.

The device is enabled with UEFI and Secure Boot. Due to this feature, you cannot boot from USB drives if you do not enter the BIOS, disable Secure Boot, change the boot mode to Legacy, and enable the **Boot from USB** option. Secure Boot is supported during the initial setup.

## Upgrading BIOS

You can upgrade the BIOS of the devices using any of the following methods:


- Using a USB drive. For more information, see—[Upgrade BIOS using USB drive](#).
- Using WMS. For more information, see—[Upgrade BIOS using WMS](#).

## Upgrade BIOS using USB drive

### About this task

To upgrade the BIOS by using the USB drive, do the following:

### Steps

1. Download the BIOS binary file and copy it to a USB drive.  
 **NOTE:** The USB drive does not have to be a bootable device.
2. Plug in the USB drive into a USB port.
3. Power on the device.

4. During device start-up, press **F12**.  
The one-time boot menu is displayed.
5. In **Other Options**, select **BIOS Flash Update**.
6. Click ... to browse to the USB drive and locate the downloaded BIOS file.
7. Select the file and click **Ok**.
8. Verify the existing system BIOS information and the BIOS update information.
9. Click **Begin Flash Update**.
10. Review the warning message and click **Yes** to proceed with the update.

## Results

The device restarts and displays a progress bar at the Dell logo screen. The device restarts again when the update is complete.

# Imaging Windows 11 IoT Enterprise LTSC 2024 devices

Custom image preparation allows you to modify the shipped image to incorporate additional application, device, environment-specific configuration and capture the same which can be deployed across the installed similar ecosystem. The custom image contains all the necessary applications, drivers, settings, and security updates that are required for the devices.

**Dell Imaging Manager** is the new imaging solution. It is enhanced to provide a faster, more efficient, and more streamlined imaging experience for the Windows 11 IoT Enterprise LTSC 2024 for Dell thin clients.

The following tools can be used to capture the prepared image:

- Dell OS Recovery Tool
- Wyse Management Suite

You can capture and deploy the custom image using any of the following:

- Using Dell Imaging Manager - USB drive. For more information, see—[USB Imaging Pre-requisites](#) and [Configure USB drive for ISO imaging or capture the recovery image on USB drive](#).
- Using WMS. For more information, see—[Imaging Windows 11 IoT Enterprise LTSC 2024 devices using WMS](#).
- Using Dell Imaging Manager - Bare Metal Recovery. For more information, see—[Bare Metal Recovery](#).

## Dell Imaging Manager

### USB Imaging Prerequisites

Follow these steps to configure your USB drive for compatibility with Dell imaging before using USB imaging:

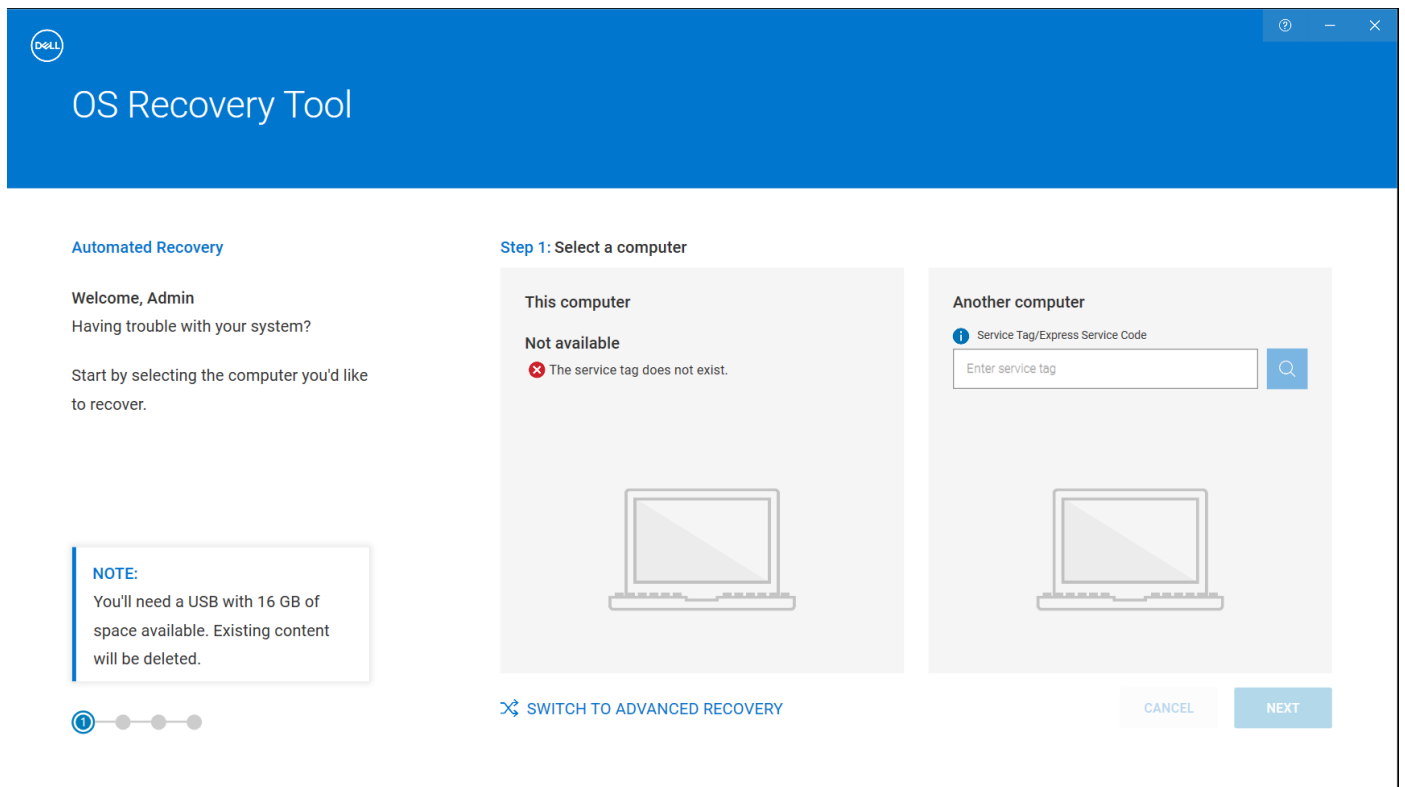
- Download the appropriate Windows 11 IoT Enterprise LTSC 2024 operating system ISO image from the [Dell | Support](#).
- Download and install the Dell OS Recovery Tool (available for Microsoft Windows only) from [Reinstall Microsoft Windows | Dell US](#).
- Use a USB flash drive with at least 32 GB of free space.
- You must have administrator user rights and at least 64 GB of available hard drive space to download the Dell operating system recovery image.
- A wired network connection is recommended for network stability.
- Disable any anti-virus software during the download.

The creation of the Recovery USB drive is complete.

### Configure USB drive for ISO imaging or capture the recovery image on USB drive

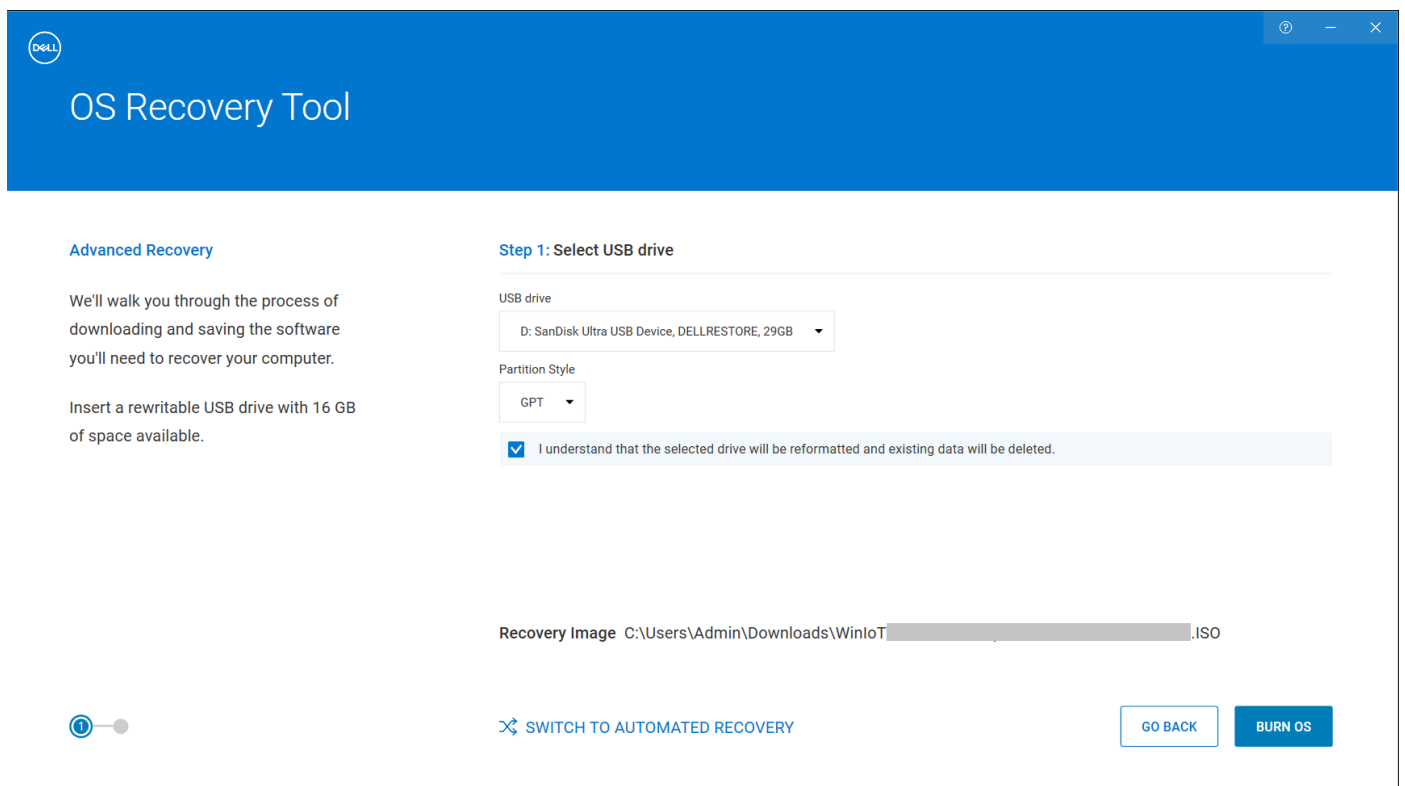
#### Steps

1. Launch the Dell OS Recovery Tool and click **INSTALL**.
2. Click **CLOSE** and launch the application from the desktop shortcut.
3. Click **SWITCH TO ADVANCED RECOVERY**.



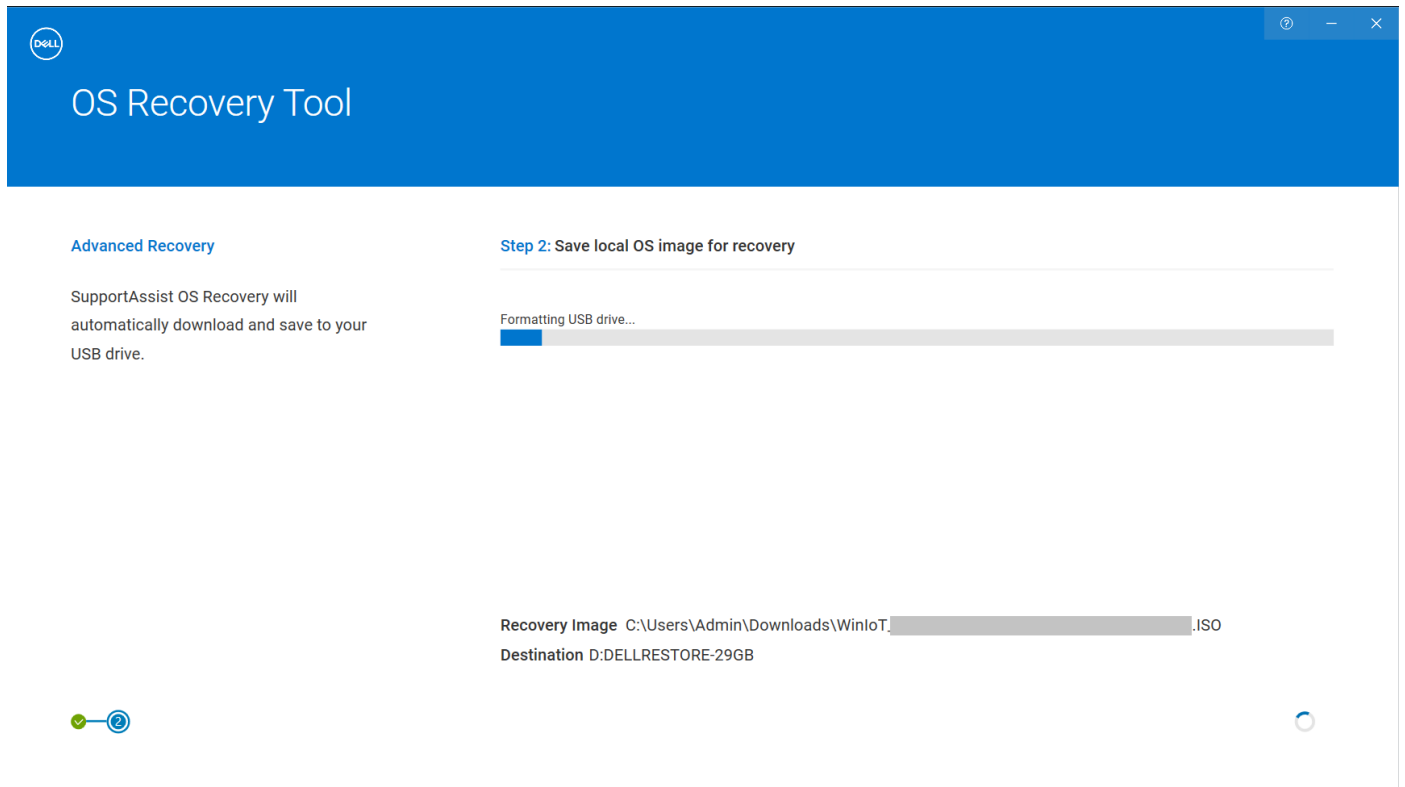
**Figure 12. OS Recovery Tool**

4. Browse to the Windows 11 IoT Enterprise LTSC 2024 ISO image, select it, and click **NEXT**.
5. Click **BURN OS**.



**Figure 13. OS Recovery Tool**

6. Wait for image registration to complete.



**Figure 14. OS Recovery Tool**

7. Click **Close**.
8. Remove the USB drive.  
The USB drive is configured with the device-specific Windows 11 IoT Enterprise LTSC 2024 image.

## Capture an image using USB

The steps below outline how to capture a golden image using a USB drive.

### Prerequisites

- The USB drive must be configured for Dell imaging. See *Configure USB drive for ISO imaging or capture the recovery image on USB drive* under the [USB Imaging Prerequisites](#).

### About this task

The following steps for USB Image Capture using Dell Imaging Manager apply only to devices running Windows 11 IoT Enterprise LTSC 2024.

**NOTE:** The recovery image is captured using the Dell OS Recovery tool. For capturing the Windows 11 IoT Enterprise LTSC 2024 e-support image, see *Configure USB drive for ISO imaging or capture the recovery image on USB drive* under the [USB Imaging Prerequisites](#).

**NOTE:** The **System Preparation Tool** generates an error during image capture. This error aborts the imaging process. This issue is specific to the Windows 11 Enterprise LTSC 2024 touchscreen devices and it is a Microsoft known issue.

Before reinitiating the imaging process, follow the steps below on the device to address this issue.

1. Log in to the device as an administrator, with the **Write Filter (WF)** disabled.
2. Using PowerShell, search for Handwriting packages: `(Get-AppxPackage -PackageTypeFilter Framework | ? {$_.PackageFullName -like "Microsoft.Ink*"}).PackageFullName`
3. Remove each package using the command: `Remove-AppxPackage -Package NAME-OF-PACKAGE`
4. Using PowerShell, search for the Handwriting.Main package: `(Get-AppxPackage -PackageTypeFilter Main | ? {$_.PackageFullName -like "Microsoft.Ink*"}).PackageFullName`

5. Remove the `Handwriting.Main` package using the command: `Remove-AppxPackage -Package NAME-OF-PACKAGE`
6. Search to confirm that all handwriting packages are removed (the output should return blank):  
(`Get-AppxPackage -PackageTypeFilter Framework | ? {$_.PackageFullName -like "Microsoft.Ink*"} .PackageFullName`)

## Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in as an administrator again.
4. Insert the configured USB drive into the device.
5. Go to **This PC**.
6. Double-click the wanted partition of the USB drive.
7. Inside the partition, double-click the **DIM\_USB** folder.
8. Launch the **DIM.USBImaging.exe** file to open the **Dell Imaging Manager** screen.
9. Click **Capture Image**.
10. Click **Create a system image** and then click **Yes, Proceed**.
11. Select a removable drive for capturing and click **Confirm**.
12. The **Create a new System Image** screen appears.

Create a new System Image

**ImageSource**

USB

☒ **Update Password** (Optional) ⓘ

<b>Admin</b>	<b>User</b>
Password	Password
<input type="password"/>	<input type="password"/>
Confirm Password	Confirm Password
<input type="password"/>	<input type="password"/>

☐ **Join a Domain** (Optional)

Cancel Capture Image

Figure 15. Create a new System Image

13. Optionally, click the checkbox **Update Password** and enter a new password for both Admin and User profiles. The password must meet the complexity criteria set on the devices where the image is restored.

**NOTE:** When the **Update Password** is not selected, use the following default password credentials for the ISO image:



- Administrator account: Admin#<Service Tag of the device>
- User account: User#<Service Tag of the device>

Replace <Service Tag of the device> with the Service Tag for your device.

14. Optionally, click the checkbox **Join a Domain** and enter the domain details to join the device to a specific domain postimaging process.

15. Click **Capture Image**.

- When you click **Capture Image**, the pre-sysprep process loads after a short delay.
- The pre-sysprep process begins and displays progress indicators for the ongoing tasks.
- The device reboots for the first time, followed by the post-sysprep process, displaying the progress indicators for the ongoing tasks.
- The device reboots after the post-sysprep process completes, and it captures the image successfully.

## Results

To verify that the image is captured:

- Log in to the device as an administrator.
- Go to the selected USB drive partition.
- Double-click the **Images** folder to check if the image is successfully captured.

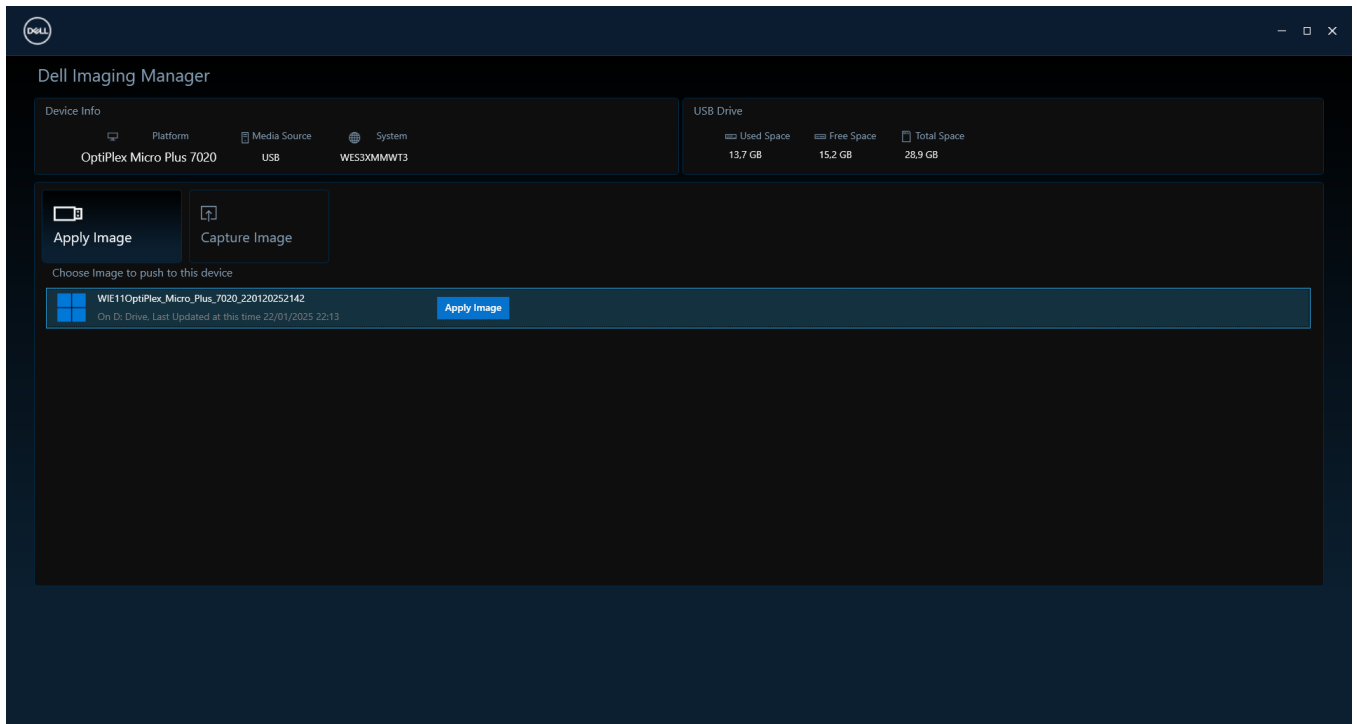
# Deploy an image using USB

## About this task

- The following steps for USB Image Deployment using Dell Imaging Manager apply only to devices running Windows 11 IoT Enterprise LTSC 2024.
- Ensure the image that is deployed on the device is captured for that device. Images from other platforms are not compatible.

## Steps

1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in to the device as an administrator again.
4. Connect the USB drive configured for ISO imaging. For more information see—[USB Imaging Prerequisites](#) and [Configure USB drive for ISO imaging or capture the recovery image on USB drive](#).
5. Go to **This PC**.
6. Double-click the wanted partition of the USB drive.
7. Inside the partition, double-click the **DIM\_USB** folder.
8. Launch the **DIM.USBImaging.exe** file to open the **Dell Imaging Manager** screen.
9. Click **Apply Image**.
10. Choose the image to deploy and select it.



**Figure 16. Dell Imaging Manager**

11. After selecting the image, click **Apply Image**.
12. Click **Confirm**.
  - When you click **Confirm**, the recovery process loads after a brief delay.
  - The device enters recovery mode and shows progress indicators for the Applying Image process. At this stage, it is safe to remove the USB drive.

## Results

- After the first reboot, the device enters the postimaging process, displaying progress indicators for all critical tasks in progress.
  - After a final reboot, the device successfully applies the Windows 11 IoT Enterprise LTSC 2024 image.
  - The device auto logs in to the **User** account.
- NOTE:** The default password credentials for the Admin and User accounts in the Windows 11 IoT Enterprise LTSC 2024 ISO image are as follows:
- **Admin:** Admin#<Service Tag of the device>
  - **User:** User#<Service Tag of the device>

## Bare Metal Recovery

When a device experiences password loss, disk failure, or another catastrophic event, this feature restores the device to its original state. You can deploy a preconfigured recovery image or custom image to reset the device, erasing any existing data and settings. The applied image restores the device to its original factory settings, allowing the user to regain access.

### Prerequisites


The USB drive can contain the ISO or recovery image or the custom image to be deployed into the bare metal device. See detailed steps in [Capture an image using USB](#) to capture the custom image or [Configure USB drive for ISO imaging or capture the recovery image on USB drive](#) to capture the recovery image.

### Steps

1. Insert the USB with the custom image or recovery image into the target device.
2. Power on the device.


3. Press **F12** to open the **One-Time Boot Settings**.
4. Click the USB drive with the custom image or recovery image under the **UEFI Boot Devices**.
5. Enter the BIOS admin password. The Dell default password is **Fireport**.
6. The device boots and opens the **Dell Imaging Manager**.
7. Click **Apply Image**. The Windows 11 IoT Enterprise LTSC 2024 image files are displayed.
8. Select the Windows 11 IoT Enterprise LTSC 2024 image.
9. Click **Apply Image**.  
The **Confirm Applying New System Image** window is displayed.
10. Click **Yes, Proceed**.  
The device enters recovery mode and shows progress indicators for the Applying Image process. At this stage, remove the USB drive. The post-imaging process will begin after a brief pause.

## Results

- After the first reboot, the device enters the postimaging process, displaying progress indicators for all critical tasks in progress.
  - After a final reboot, the device successfully applies the image and upgrades to Windows 11 IoT Enterprise LTSC 2024.
  - The device auto logs in to the User account.
-  **NOTE:** The default password credentials for the Admin and User accounts in the Windows 11 IoT Enterprise LTSC 2024 ISO image are as follows:
- **Admin:** Admin#<Service Tag of the device>
  - **User:** User#<Service Tag of the device>


# Troubleshooting

To view windows and other program messages, use Event Viewer. In the **Component Services** console, click the **Event Viewer** icon from the **Console Root** tree. The summary of all the logs of the events that have occurred on your device is displayed. For more information, see [Event Viewer](#).

 **NOTE:** Event logs are cleared when the device reboots due to Write Filter.

## Capturing logfiles

To collect different types of logs for an application, configure the `DebugLog.xml` file. Modify log levels within this file to specify the required log details. Log files are generated in the following location: `C:\Windows\Logs\<Application name>\Logs`

 **NOTE:** Log file creation is disabled by default.

## Configuration of DebugLog XML file

The Debug Configuration Editor (DCE) console application provides tools to manage the `DebugLog.xml` file to commit, exclude, or modify the debug configuration file.

To commit, exclude, or modify the debug configuration file, enter the following commands on the Debug Configuration Editor:

- To commit the file and obtain the log files—`DebugConfigEditor.exe -CommitLog -Path "DebugLog.xml"`. This command commits the file present in the path that is mentioned in `Debug.xml`.
- To exclude the collection of logs from a folder mentioned in the `Debug.xml`—`DebugConfigEditor.exe -ExcludeLog -Path "DebugLog.xml"`.
- To configure the `Debug.xml` file to collect different types of logs—`DebugConfigEditor.exe -UpdateConfig -Path "DebugLog.xml" -LogPath "Path of Log File" -LogFileName "Name of log File" -LogLevel "logLevel"`.

The following table describes the different `LogLevel` values that can be used:

**Table 18. LogLevel values**

Value	Description
0	Logs are not captured.
1	Error logs are captured.
2	Warning logs are captured.
3	Error and warning logs are captured.
4	Information logs are captured.
7	All logs are captured.

## Request a log file using WMS

### Steps

1. Log in to WMS as an administrator.
2. Go to the **Devices** page, and click a particular device.

The **Device Details** page is displayed.

3. Click the **Device Log** tab.
4. Click **Request Log File**.  
An **Alert** window is displayed.
5. Click **Send Command**.
6. After the log files are uploaded to the WMS server, click the **Click here** link, and download the logs.


## View audit logs using WMS

### Steps

1. Log in to WMS as an administrator.
2. Go to **Events > Audit**.
3. From the **Configuration Groups** drop-down list, select a group for which you want to view the audit log.
4. From the **Timeframe** drop-down list, select the time period to view the events that occurred during that time period.  
The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

## Viewing events


To view monitoring and troubleshooting messages from Windows and other programs, use the Event Viewer window. In the Component Services console, click the **Event Viewer** icon from the **Console Root** tree. The summary of all the logs of the events that have occurred on your computer is displayed. For more information, see [Event Viewer](#).

 **NOTE:** Event logs are lost on reboot because of Write Filter.

## Capture and locate the log files of an application

Locating and capturing log files of an application is a crucial step in debugging, troubleshooting, or monitoring its performance.

You must enable the capture of the log files of different applications using the following methods:

-  **NOTE:**
- You must log in as an administrator and enable the capture of log files for various applications when the **WF** is disabled.
  - **Wyse Device Agent (WDA)** – To enable the capture of WDA log files, do the following:
    1. Open the WDA application.
    2. Go to **Support** and enable the **Support Mode** option.  
The logs are captured in the WyseDeviceAgent log file at C:\Wyse\WDA.
  - **Wyse Easy Setup** – To enable the capture of Wyse Easy Setup log files, do the following:
    1. Go to **Start > Wyse > WyseEasySetupAdmin**. The Wyse Easy Setup user interface is displayed.
    2. In **Debug Log**, click **Enable DebugLog**.  
The logs are captured in C:\Wyse\WDA\WyseEasySetup.
  - **Application Launch Manager (ALM)** – To enable the capture of ALM log files, do the following:
    1. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.
    2. On the left navigation bar, go to **UTILITIES > Application Launch Manager**.
    3. Select the **Enable DebugLog** option.  
The logs are captured in the ALMLog log file at C:\Wyse\WAPPS\ALM.
  - **Extra Data Cleanup Manager (xDCM)** – To enable the capture of xDCM log files, do the following:
    1. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.
    2. On the left navigation bar, go to **UTILITIES > Extra Data Cleanup Manager**.
    3. Select the **Enable DebugLog** option.  
The log files are captured in the XDCMLog folder at C:\Wyse\WAPPS\XDCM.

The log files that are related to imaging, custom Sysprep, and Dell Application Control Center installation are created at C:\Wyse\WAPPS.

# Viewing and exporting operating system image manifest files

A manifest file is an xml document which contains metadata about the operating system image. By comparing the current manifest with the original factory manifest, you can identify changes made to the device. The following are the two types of manifest files that are based on the source of data collection:

**Table 19. Manifest files**


Manifest Source	Installed Products	QFE	Drivers
Current Manifest	Yes	Yes	Yes
Factory Manifest	Yes	Yes	Yes

Installed products, QFE, and driver details from current and the factory manifest files can be compared to find the change on the device regarding the installed applications, QFEs, and drivers respectively.

## View and export operating system image current manifest information

### Steps


1. Log in to the device as an administrator.
2. Disable the **WF**:  
Double-click the **Dell Wyse WF Disable** icon on the desktop.  
The Write Filter is disabled and the device restarts.
3. Log in as an administrator.
4. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.  
The **Application Control Center** window is displayed.
5. On the left navigation bar, go to **UTILITIES**.
6. In the **Capture Manifest** section, click **Export Support Data**.  
The data is exported to the default path `C:\Wyse\WAPPS\DellTCASupportInfo\Logging\`.

 **NOTE:** To choose a custom folder, select **Custom Path** and browse to the required folder.

## View operating system image factory manifest information

### Steps

1. Log in to the device as an administrator.
2. Go to `C:\Windows\Setup\Tools`.  
The `BuildContent` folder contains the factory manifest of the device.
3. View the information of the operating system image manifest.
  - To view the information of the installed products in the factory at the time of shipment, go to **Apps > InstalledProducts xml file**.
  - To view the information of the QFEs installed in the factory at the time of shipment, go to **Qfe > QFE xml file**.
  - To view the information of the recently installed drivers manifest information, go to **Drivers > Drivers xml file**.

 **NOTE:**

- You can compare the **InstalledProducts**, **QFE**, and **Drivers** .xml files that are generated through the Application Control Center with the .xml files present in the `C:\Windows\Setup\Tools\BuildContent` folder. This comparison helps you identify changes that are related to the installed applications and QFEs.
- You can share the **support data** and the **build content** data with the support team during troubleshooting.

# Error message while importing Wyse Easy Setup configurations from WMS

The following types of warnings can be displayed while importing Wyse Easy Setup configurations from WMS:

- **Imported <device type> policies will be applied to group <group name>**—This warning is displayed when you import the device type configurations to a group that does not contain any of these device type configurations.
- **<Device type> policies already exists for the <group name> group. Existing <device type> policies will be removed and imported policies will be applied**—This warning is displayed when you import the device type configurations to a group that contains the device type configurations.
- **Importing policies from a file that contains dependencies to inventory files will fail. To allow this import, use the import option from the Edit Policies window**—This warning is displayed when you import the device type configurations from a file that contains references to inventory files.

## Keyboard customization issues

To customize the keyboard language that is not supported by default, do the following:

1. Go to `C:\Windows\system32\oobe`.
2. Delete the `oobe.xml` file and the related subdirectories.
3. Manually modify the `sysprep.xml` file to specify the required keyboard layout, locale, and other language preferences.
4. Deploy the updated `sysprep.xml` file using either Microsoft Endpoint Configuration Manager or a custom Sysprep.

Once completed, the system reflects the chosen keyboard, locale, time zone, and country settings.

## Frequently asked questions

### How to set up a smart card reader?

To set up a smart card reader, do the following:

1. Log in to the device as an administrator.
2. Disable the **WF**: Double-click the **Dell Wyse WF Disable** icon on the desktop. The Write Filter is disabled and the device restarts.
3. Download your preferred smart card application.
4. Extract the file to your local drive.
5. Connect the smart card reader with the smart card, and click **Setup**.
6. After the installation is complete, install the server certificate if you want to establish a connection for Citrix or VMware setup.
7. Enable Unified Write Filter.
8. Connect to your preferred VDI session such as Citrix, VMware, or RDP.

### How to use USB Redirection?

USB Redirection enables you to connect a peripheral into a USB port on your device and access the device using a remote desktop or application.

You configure USB Redirection in a Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) environment. For more information, see Citrix Generic USB redirection and client drive considerations in Citrix product documentation.

You also configure options to use and manage USB devices in a VMware Horizon virtual desktop session. For more information, see Use USB Devices on Horizon Windows Client in Omnisia documentation.

### How to add an application package to the WMS repository?

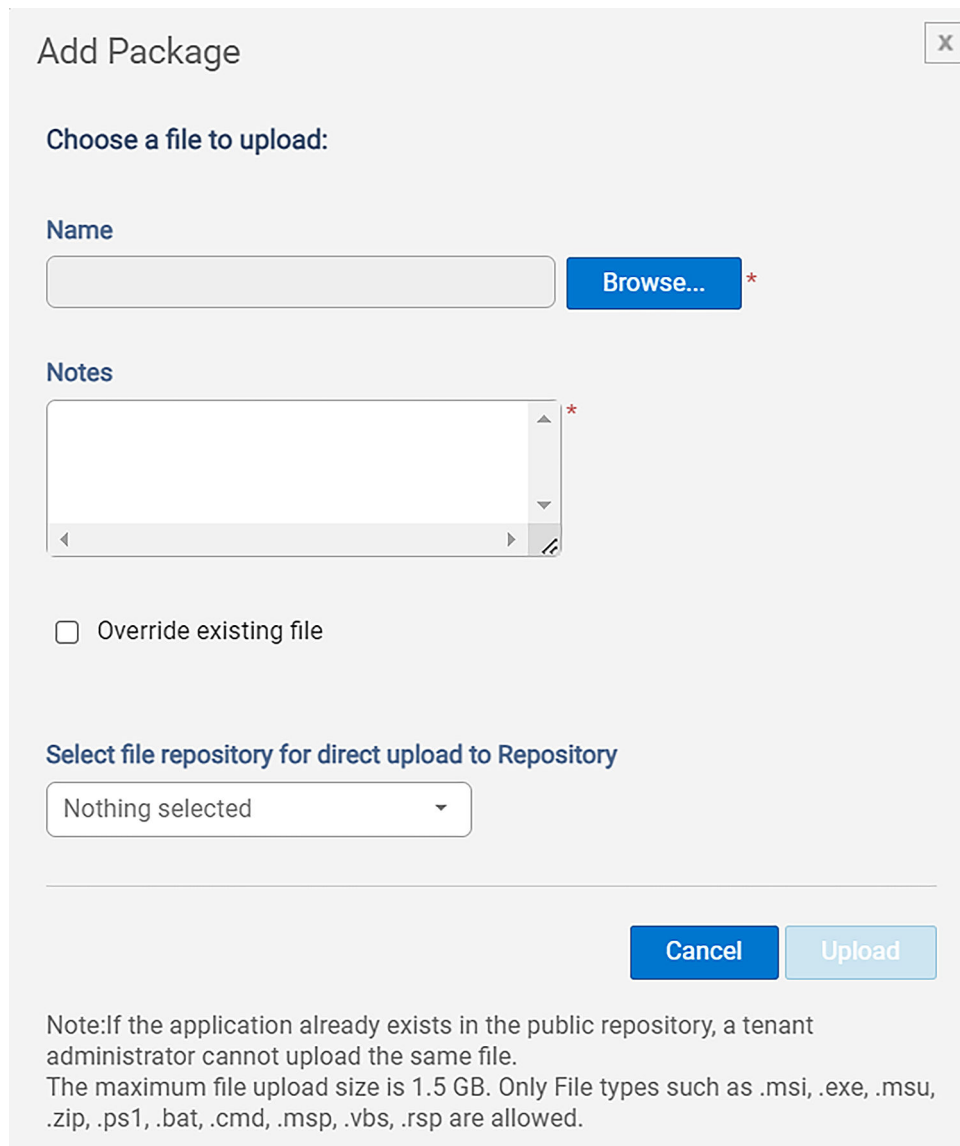
#### Prerequisites

- 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**

Choose a file to upload:

Name

Browse...

Notes

☐ Override existing file

Select file repository for direct upload to Repository

Nothing selected

Cancel Upload

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 17. 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.

## Can I configure Wyse Easy Setup locally on the device which is managed by WMS?

You cannot configure Wyse Easy Setup locally on the device which is managed by WMS. The Wyse Easy Setup user interface is disabled.

## How do I import the local Wyse Easy Setup configurations to WMS?

To import local Wyse Easy Setup configurations to WMS, see [Import Wyse Easy Setup configurations from WMS](#).

## Can I host operating system images in the WMS cloud repository?

You cannot host operating system images in the WMS cloud repository since the free space that is provided in the WMS cloud repository is only 5 GB.

# End User License Agreement (EULA)

This section outlines the terms and conditions for software usage, including licensing rights, restrictions, and limitations of liability. You can find the Dell EULA at [Dell End User License Agreement](#). The following sections capture the EULA of different third party applications:

- Amazon WorkSpaces—[Amazon WorkSpaces Application License Agreement](#).
- VMware Horizon Client—[VMWARE END USER LICENSE AGREEMENT](#).
- Cisco—[Cisco General Terms](#).
- Citrix Workspace App—[Citrix Workspace End User License Agreement](#).
- Microsoft—[Microsoft Software License Terms](#).

## Dell End User License Agreement

This document contains the terms and conditions for the use of Dell products and software.

Congratulations on your new Dell purchase!

Your purchase and use of this product is subject to and governed by Dell's applicable Terms of Sale and End User License Agreement, which are each presented below in the following order:

- Terms of Sale Websites
- End User License Agreement

In addition, please take note of the important Safety Information.

By the act of clicking **I accept**, you agree (or re-affirm your agreement to) the foregoing terms and conditions and acknowledge that you have read and understood the Safety Information. For the avoidance of doubt, to the extent that Dell is deemed under applicable law to have accepted an offer by you: (a) Dell hereby objects to and rejects all additional or inconsistent terms that may be contained in any purchase order or other documentation submitted by you in connection with your order; and (b) Dell hereby conditions its acceptance on your assent that the foregoing terms and conditions shall exclusively control.

IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT USE THIS PRODUCT AND CONTACT YOUR DELL REPRESENTATIVE WITHIN FIVE BUSINESS DAYS TO ARRANGE A RETURN.

---

### Safety Information

**WARNING:** To help avoid risk of bodily injury or property damage, observe the following warnings:

#### Battery Safety

- Use only a battery obtained from Dell and approved for use with this device. Using a battery from a third-party source may increase the risk of fire.
- Fully discharge the battery in the device prior to servicing, replacing or removal for recycling, return or disposal. Handle battery with care. Do not disassemble the battery. A damaged battery may pose a risk of personal injury or fire.

#### Power and Adapter Safety

- Use only a Dell-provided AC adapter approved for use with this device.
- Do not allow your computer or adapter to rest directly on exposed skin for extended periods of time. Sustained contact with exposed skin can cause discomfort or burn.

#### Electrical Safety

- Before you connect the equipment to an electrical outlet, ensure that the equipment voltage and frequency rating match the available power source.
- Plug the equipment power cables into properly grounded electrical outlets, and use only the approved power cables rated for the equipment.

See Safety and Regulatory Content in [dell.com/regulatory\\_compliance](http://dell.com/regulatory_compliance) for additional safety and regulatory information.

#### Terms of Sale Websites

If you purchased directly from Dell for your internal use, your purchase is governed by the applicable Terms of Sale, unless you have a separate written agreement with Dell that specifically applies to your order.

#### AMERICAS

- US: [www.dell.com/terms](http://www.dell.com/terms)
- Canada: [Dell.ca/terms](http://Dell.ca/terms)
- Canada (French): [Dell.ca/conditions](http://Dell.ca/conditions)
- Argentina: [www.dell.com/es-ar/lp/legal/terms-of-sale](http://www.dell.com/es-ar/lp/legal/terms-of-sale)
- Aruba: [www.dell.com/en-aw/lp/legal/terms-of-sale](http://www.dell.com/en-aw/lp/legal/terms-of-sale)
- Bahamas: [www.dell.com/en-bs/lp/legal/terms-of-sale](http://www.dell.com/en-bs/lp/legal/terms-of-sale)
- Barbados: [www.dell.com/en-bb/lp/legal/terms-of-sale](http://www.dell.com/en-bb/lp/legal/terms-of-sale)
- Belize: [www.dell.com/en-bz/lp/legal/terms-of-sale](http://www.dell.com/en-bz/lp/legal/terms-of-sale)
- Bolivia: [www.dell.com/es-bo/lp/legal/terms-of-sale](http://www.dell.com/es-bo/lp/legal/terms-of-sale)
- Brazil: [www.dell.com/pt-br/lp/legal/terms-of-sale](http://www.dell.com/pt-br/lp/legal/terms-of-sale)
- Chile: [www.dell.com/es-cl/lp/legal/terms-of-sale](http://www.dell.com/es-cl/lp/legal/terms-of-sale)
- Colombia: [www.dell.com/es-co/lp/legal/terms-of-sale](http://www.dell.com/es-co/lp/legal/terms-of-sale)
- Costa Rica: [www.dell.com/es-cr/lp/legal/terms-of-sale](http://www.dell.com/es-cr/lp/legal/terms-of-sale)
- Ecuador: [www.dell.com/es-ec/lp/legal/terms-of-sale](http://www.dell.com/es-ec/lp/legal/terms-of-sale)
- El Salvador: [www.dell.com/es-sv/lp/legal/terms-of-sale](http://www.dell.com/es-sv/lp/legal/terms-of-sale)
- Guatemala: [www.dell.com/es-gt/lp/legal/terms-of-sale](http://www.dell.com/es-gt/lp/legal/terms-of-sale)
- Haiti: [www.dell.com/en-ht/lp/legal/terms-of-sale](http://www.dell.com/en-ht/lp/legal/terms-of-sale)
- Honduras: [www.dell.com/es-hn/lp/legal/terms-of-sale](http://www.dell.com/es-hn/lp/legal/terms-of-sale)
- Mexico: [www.dell.com/es-mx/lp/legal/terms-of-sale](http://www.dell.com/es-mx/lp/legal/terms-of-sale)
- Panama: [www.dell.com/es-pa/lp/legal/terms-of-sale](http://www.dell.com/es-pa/lp/legal/terms-of-sale)
- Paraguay: [www.dell.com/es-py/lp/legal/terms-of-sale](http://www.dell.com/es-py/lp/legal/terms-of-sale)
- Peru: [www.dell.com/es-pe/lp/legal/terms-of-sale](http://www.dell.com/es-pe/lp/legal/terms-of-sale)
- Uruguay: [www.dell.com/es-uy/lp/legal/terms-of-sale](http://www.dell.com/es-uy/lp/legal/terms-of-sale)
- Venezuela: [www.dell.com/es-ve/lp/legal/terms-of-sale](http://www.dell.com/es-ve/lp/legal/terms-of-sale)

#### EUROPE

- Austria: [www.dell.at/Geschaeftsbedingungen](http://www.dell.at/Geschaeftsbedingungen)
- Belgium (Dutch): [www.dell.be/voorwaarden](http://www.dell.be/voorwaarden)
- Belgium (French): [www.dell.be/ConditionsGeneralesdeVente](http://www.dell.be/ConditionsGeneralesdeVente)
- Czech: [www.dell.cz/podminky](http://www.dell.cz/podminky)
- Denmark: [www.dell.dk/salgsbetingelser](http://www.dell.dk/salgsbetingelser)
- Finland: [www.dell.fi/myyntiehtdot](http://www.dell.fi/myyntiehtdot)
- France: [www.dell.fr/ConditionsGeneralesdeVente](http://www.dell.fr/ConditionsGeneralesdeVente)
- Germany: [www.dell.de/Geschaeftsbedingungen](http://www.dell.de/Geschaeftsbedingungen)
- Greece: [www.dell.gr/terms](http://www.dell.gr/terms)
- Ireland: [www.dell.ie/terms](http://www.dell.ie/terms)
- Italy: [www.dell.it/condizionigeneralidivendita](http://www.dell.it/condizionigeneralidivendita)
- Luxembourg: [www.dell.lu/ConditionsGeneralesdeVente](http://www.dell.lu/ConditionsGeneralesdeVente)
- Netherlands: [www.dell.nl/voorwaarden](http://www.dell.nl/voorwaarden)
- Norway: [www.dell.no/salgsbetingelser](http://www.dell.no/salgsbetingelser)
- Poland: [www.dell.pl/warunki](http://www.dell.pl/warunki)
- Portugal: [www.dell.pt/ClausulasContratuaisGerais](http://www.dell.pt/ClausulasContratuaisGerais)
- Slovakia: [www.dell.sk/podmienky](http://www.dell.sk/podmienky)
- South Africa: [www.dell.co.za/terms](http://www.dell.co.za/terms)
- Spain: [www.dell.es/CondicionesGeneralesdeContratacion](http://www.dell.es/CondicionesGeneralesdeContratacion)
- Sweden: [www.dell.se/forsaljningsvillkor](http://www.dell.se/forsaljningsvillkor)
- Switzerland (French): [www.dell.ch/termesetconditions](http://www.dell.ch/termesetconditions)
- Switzerland (German): [www.dell.ch/Geschaeftsbedingungen](http://www.dell.ch/Geschaeftsbedingungen)
- UK: [www.dell.co.uk/terms](http://www.dell.co.uk/terms)

#### ASIA and OCEANIA

- Mainland China: [www.dell.com/zh-cn/lp/legal/terms-of-sale](http://www.dell.com/zh-cn/lp/legal/terms-of-sale)
- Hong Kong: [www.dell.com/zh-hk/lp/legal/terms-of-sale](http://www.dell.com/zh-hk/lp/legal/terms-of-sale)
- Taiwan: [www.dell.com/zh-tw/lp/legal/terms-of-sale](http://www.dell.com/zh-tw/lp/legal/terms-of-sale)

- Singapore: [www.dell.com/en-sg/lp/legal/terms-of-sale](http://www.dell.com/en-sg/lp/legal/terms-of-sale)
- Malaysia: [www.dell.com/en-my/lp/legal/terms-of-sale](http://www.dell.com/en-my/lp/legal/terms-of-sale)
- Thailand: [www.dell.com/en-th/lp/legal/terms-of-sale](http://www.dell.com/en-th/lp/legal/terms-of-sale)
- Australia: [www.dell.com/en-au/lp/legal/terms-of-sale](http://www.dell.com/en-au/lp/legal/terms-of-sale)
- New Zealand: [www.dell.com/en-nz/lp/legal/terms-of-sale](http://www.dell.com/en-nz/lp/legal/terms-of-sale)
- India: [www.dell.com/en-in/lp/legal/terms-of-sale](http://www.dell.com/en-in/lp/legal/terms-of-sale)
- Korea: [www.dell.com/ko-kr/lp/legal/terms-of-sale](http://www.dell.com/ko-kr/lp/legal/terms-of-sale)
- Japan: [www.dell.com/ja-jp/lp/legal/terms-of-sale](http://www.dell.com/ja-jp/lp/legal/terms-of-sale)

Translated versions may be found at [www.dell.com/eula\\_translations](http://www.dell.com/eula_translations)

## End User License Agreement

This End User License Agreement ("EULA") is between the individual consumer or business entity that will use the Software ("You") and the applicable entity identified in the "Licensor Table" located at [www.dell.com/swlicensortable](http://www.dell.com/swlicensortable) ("Licensor").

This EULA governs Your use of:

- the object code version of Dell branded software that is preinstalled on Dell hardware or otherwise provided to You pursuant to a purchase contract, quote, order form, invoice or online procurement process (each, an "Order");
- associated software license keys, if any ("License Keys");
- updates to such software ("Updates");
- the documentation for such software; and
- all copies of the foregoing (collectively, "Software").

If You accept this EULA, or if You install or use the Software, then You agree to this EULA unless You already have a signed agreement with Dell Marketing L.P. or one of its affiliates ("Dell") that includes licensing terms that govern Your use of the Software ("Pre-Existing Agreement"). If You accept this EULA or install or use the Software on behalf of a business entity, then You represent that You have authority to take those actions, and this EULA will be binding on that business entity unless the entity already has a Pre-Existing Agreement. If You do not agree to this EULA, do not install or use the Software.

If You are a business entity and You purchase Software from a third party ("Reseller") who sublicenses the Software to You under the terms of an agreement between You and such Reseller (a "Sublicense Agreement"), then the terms of Your Sublicense Agreement with the Reseller shall govern Your use of the Software and not this EULA. Resellers may only grant rights, and must pass through conditions, consistent with this EULA. Thus, even though Your Sublicense Agreement is between you and the Reseller, by installing or using the Software, You acknowledge and agree that:

- any license rights in the Sublicense Agreement that are greater than the license rights in this EULA shall not apply;
- any license conditions in this EULA that are not contained in the Sublicense Agreement apply to You;
- the limitations of liability set forth in this EULA will apply in favor of Licensor, its affiliates and suppliers despite the existence of a Sublicense Agreement; and
- Licensor is a third-party beneficiary of the Sublicense Agreement and is entitled to exercise and enforce all of the Reseller's rights and benefits under that Sublicense Agreement.

If You purchase Software as an individual consumer, nothing in this EULA affects your statutory rights if the laws of your state or country do not permit it to do so.

### 1. License Grant.

1.1. Right to Use. Subject to and in consideration of your full compliance with the terms and conditions of this EULA, Licensor grants to You a personal, non-exclusive license to use the Software during the period stated in the applicable Order (if no period is specified, You may use the Software perpetually). If You are an individual consumer, this license grant allows You to use the Software in connection with Your own personal use. If You are a business entity, this license grant allows You to use the Software in connection with the internal business operations of Your entity. In addition, You may make a reasonable number of copies of the Software solely as needed for backup or archival purposes. Additional license terms for certain Software may be included in the Offering Specific Terms Table located at [www.dell.com/offeringspecificterms](http://www.dell.com/offeringspecificterms) ("OST Table"), and additional terms for Software that is licensed to You for a limited time ("Subscription Software") are located at [www.delltechnologies.com/subscription\\_terms](http://www.delltechnologies.com/subscription_terms) ("Subscription Terms").

1.2. Third Party Use. If You are a business entity, You may allow Your contractors (each, a "Permitted Third Party") to use the Software solely for the purpose of providing services to You, provided that such use is in compliance with this EULA. You are liable for any breach of this EULA by any Permitted Third Party.

1.3. Rights Reserved. The Software is licensed and not sold. Except for the license expressly granted in this EULA, Licensor, on behalf of itself and its affiliates and suppliers, retains all rights in and to the Software and in all related materials ("Works"). The rights in these Works are valid and protected in all forms, media and technologies existing now or hereafter developed. Any use of Works other than as expressly set forth herein is strictly prohibited.

1.4. Ownership. Licensor, on behalf of itself and its affiliates, retains ownership of the Works and all related intellectual property rights. If Software is provided to You on removable media (e.g., CD, DVD or USB drive), You may own the media on which the Software is recorded.

## 2. License Conditions.

### 2.1. You and Your Permitted Third Parties must do the following:

A. Run the Software only on the hardware for which it was intended to operate, when applicable;

B. Use License Keys (if applicable) only from Licensor or an authorized Dell License Key provider;

C. Treat the Software as Dell confidential information;

D. Use the Software only on as many computers or devices that You purchased, in such configurations permitted by Dell or Licensor, and/or in accordance with the applicable unit of measure, each as may be specified on Your Order. For Software licensed via a unit of measure, the terms and descriptions of each unit of measure are located at [www.delltechnologies.com/UOM\\_terms](http://www.delltechnologies.com/UOM_terms) ("UOM Terms");

E. Abide and be responsible for compliance with the export control and economic sanctions laws of the United States, the European Union, and other applicable jurisdictions (collectively, "Applicable Trade Laws"). Software, including any associated intellectual property rights or trade secrets that may accompany it, may not be used, licensed, sold, supplied, leased, exported, imported, re-exported, or transferred, whether directly or indirectly, to restricted countries (including, but not limited to Cuba, Iran, North Korea, Syria, Russia, Belarus, and the Crimea, Donetsk, and Luhansk regions of Ukraine), restricted end users, or for restricted end uses according to the Applicable Trade Laws. Dell reserves all rights and remedies to enforce these restrictions, including injunctive relief, damages, and cancellation/termination of this EULA. You represent and warrant that You or Your Permitted Third Parties are not the subject or target of, or located in a country or territory that is the subject or target of economic sanctions under the Applicable Trade Laws. For further information about geographical restrictions and compliance with Applicable Trade Laws, visit [www.dell.com/tradecompliance](http://www.dell.com/tradecompliance); and

F. Comply with all Third Party Terms (as defined in Section 5 below).

### 2.2. Except as otherwise permitted by this EULA or by mandatory law (meaning a law that the parties cannot change by contract), You must not, and must not allow Your Permitted Third Parties, to do the following:

A. Modify or remove any proprietary notices or markings on or in the Software;

B. Transfer License Keys to any other person or entity;

C. Download Updates from Licensor or an authorized provider unless You have a valid support agreement;

D. Install Updates on Enterprise Products (e.g., server, networking, storage, integrated solutions, and data protection appliances) that have gone end of service life unless Licensor otherwise agrees in writing;

E. Install and operate counterfeit versions of Software (i.e. software provided by anyone other than Dell or an authorized representative of Dell) on Dell hardware;

F. Violate or circumvent any technological use restrictions in the Software;

G. Sell, loan, rent, lease, sublicense, distribute or encumber (e.g., by lien, security interest, etc.) the Software;

H. Use any trademarks or service marks of Licensor, its affiliates or suppliers;

I. Provide access to the Software or allow use by any third party, other than Permitted Third Parties, without Licensor's prior written consent;

J. Copy, republish, upload, post or transmit the Software in any way;

K. Modify or create derivative works based upon the Software, or decompile, disassemble, reverse engineer, or otherwise attempt to derive source code from the Software, in whole or in part;

L. Attack or attempt to undermine the security, integrity, authentication or intended operation of the Software;

M. Use the Software on a service bureau, rental or managed services basis;

N. Create or permit others to create Internet "links" to the Software or "frame" or "mirror" the Software on any other server, wireless or Internet-based device;

O. Use the Software to create a competitive offering;

P. Use the Software to create other software, products or technologies unless the Software contains Development Tools as described in Section 7;

Q. Share or publish the results of any benchmarking of the Software without Dell's prior written consent;

R. Use the Software for high risk activities, including without limitation online control systems, or use in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communications systems, air

traffic control, life support, weapons systems or in any other device or system in which function or malfunction of the Software could result in death, personal injury or physical or environmental damage;

S. Use the Software for activities related to weapons of mass destruction, including but not limited to, activities related to the design, development, production or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or support of missile projects, or chemical or biological weapons; and

T. Assign this EULA, or any right or obligation under this EULA, or delegate any performance, without Dell's prior written consent, unless You are transferring the Software in accordance with the Transferability Section 3 below. Even if Dell consents to an assignment, You remain responsible for all obligations under this EULA that You incurred prior to the effective date of the assignment.

3. **Transferability.** If You are an individual consumer, You may transfer the Software on a permanent basis as part of the sale or transfer of the hardware system on which the Software is loaded, provided that You retain no copies of any version of the Software. If You are a business entity, You may not transfer the Software to another person or entity without the express written permission of Dell, unless allowed by applicable law stating that transfer may not be restricted (note that a transfer fee may be charged by Dell).

4. **Compliance Verification.** If You are a business entity, You must: (a) maintain and use systems and procedures that allow You to accurately track Your use of the Software; (b) certify to Dell in writing, at Dell's request, that Your use of Software fully complies with this EULA, indicating the number of Software licenses deployed at that time; and (c) cooperate fully and timely with Dell and its auditors if Dell notifies You that it will conduct an audit to confirm Your compliance with this EULA. Any such audit will be conducted during normal business hours. If Dell determines that You have over-deployed Software, You agree to immediately purchase licenses at the then-current list price to bring Your use into compliance. If You over-deployed Software by 5% or more, then You agree to pay the total cost of the audit, in addition to any other liabilities You may have.

5. **Third Party Software.** "Third Party Software" is software, including open source software, that is contained in or provided with the Software and is licensed by a third party under its own terms of use ("Third Party Terms"). Third Party Software is governed solely by the applicable Third Party Terms and not by this EULA. Third Party Terms may be provided with the Third Party Software or may be included in the OST Table. For certain open source software, the applicable Third Party Terms may entitle You to obtain the corresponding source files. You may find corresponding source files for such open source software at <https://opensource.dell.com/> or in the "About" or "Read Me" file of Software, or other locations that Licensor may specify.

6. **Free Software.** "Free Software" means Software that is provided to You without additional charge (e.g., scripts that enable customer installation; code that enables You to monitor Your use of Dell products; etc.). You may only use Free Software on or with equipment or in the operating environments for which Dell has designed that Free Software to operate. Licensor may terminate any license to Free Software at any time in its sole discretion. You may not transfer Free Software to anyone else.

7. **Development Tools.** If the Software includes development tools, such as scripting tools, APIs or sample scripts (collectively "Development Tools"), and unless there is a separate agreement between You and Dell or Licensor for the Development Tools, You may use such Development Tools to create new scripts and code for the purpose of customizing Your use of the Software (within the parameters set forth in this EULA and in the Development Tools themselves) and for no other purpose.

8. **Evaluation Software.** This EULA does not license use of Software for evaluation purposes ("Evaluation Software") except to the extent these terms may be invoked by the separate license terms and conditions accompanying that Evaluation Software.

9. **Support Services Not Included.** If You purchase maintenance and support for Software, such services are identified in Your Order and will be provided under a separate services agreement.

10. **Termination.** For Subscription Software, this EULA automatically terminates at the end of Your subscription period unless You renew Your rights. Licensor may terminate this EULA if You or a Permitted Third Party commits a material breach of this EULA and fails to cure such breach within thirty (30) days following Your receipt of notice of the breach from Dell. This right to terminate applies accordingly if Dell or the Reseller from whom You made Your purchase does not receive timely payment for the licenses to the Software or for the hardware on which the Software is loaded, if any. When this EULA terminates, all licenses granted automatically terminate and You must immediately cease use of the Software and return or destroy all copies of the Software. Except as otherwise agreed by Dell, You will not get a refund from Dell if this EULA is terminated. Rights and obligations under Sections of this EULA that, by their nature should survive, will survive termination, as well as obligations for payment.

11. **Warranty Disclaimer.** Under this EULA, Licensor provides neither any warranties for the Software nor does it provide support for the Software. Your rights under any warranties and any support entitlements for Software acquired for a fee are solely between You and the Reseller or Dell entity from whom You procured the Software and related support, and are defined under the commercial terms agreed between You and such selling entity. Accordingly, except as otherwise offered by Dell, the Software is provided by Licensor under this EULA "As Is" without any warranties or conditions. To the maximum extent permitted by applicable law, Licensor, on behalf of itself and its affiliates and suppliers: (a) makes no express warranties or conditions related to the Software; (b) disclaims all implied warranties and conditions related to the Software, including merchantability, fitness for a particular purpose, title, and non-infringement; and (c) disclaims any warranty or condition arising by statute, operation of law, course of dealing or performance, or usage of trade. Licensor does not warrant uninterrupted or error-free operation of the Software. This Section does not affect or modify any of the statutory warranty rights that are available to consumers.

## 12. Limitation of Liability.

12.1. Limitations on Damages. The limitations, exclusions and disclaimers set forth in a Pre-Existing Agreement or Dell Terms of Sale that applies your Order (in each case, the "Order Terms") shall apply to all disputes, claims or controversies (whether in contract, tort or otherwise) between You and Licensor or Dell related to or arising out of: (a) this EULA; (b) the breach, termination or validity of this EULA; or (c) any Orders (each, a "Dispute"). In the absence of applicable Order Terms, the terms set forth in this Section shall apply to all Disputes.

The terms of this Section are agreed allocations of risk constituting part of the consideration for Licensor's licensing of Software to You and will apply even if there is a failure of the essential purpose of any limited remedy, and regardless of whether a party has been advised of the possibility of the liabilities. If applicable law prohibits any portion of the limits on liability stated below, the parties agree that such limitation will be automatically modified, but only to the extent required to make the limitation compliant with applicable law.

A. Limitation on Direct Damages. Except for Your obligation to pay for the Software, or for Your violation of the License Grant and License Conditions set forth herein or of Licensor's or Dell's intellectual property rights, the total liability of You and Licensor (including Licensor's affiliates and suppliers) arising out of any Dispute is limited to the amount You paid for the Software that is the subject of the Dispute, but excluding amounts received as reimbursement of expenses or payment of taxes. Notwithstanding anything otherwise set forth above, Licensor and its affiliates have no liability for any direct damages resulting from Your use or attempted use of Third Party Software, Free Software or Development Tools.

B. Disclaimer of Certain Other Damages. Except for Your obligation to pay for the Software, or for Your violation of the License Grant and License Conditions set forth herein or of Licensor's or Dell's intellectual property rights, neither You nor Licensor (including Licensor's affiliates and suppliers) shall have any liability under this EULA for special, consequential, exemplary, punitive, incidental or indirect damages, or for lost profits, loss of revenue, loss or corruption of data, loss of use or procurement of substitute products or services.

12.2. Regular Backups. You are solely responsible for Your data. You must back up Your data before Licensor or a third party performs any remedial, upgrade or other work on Your production systems. You acknowledge that it is a best practice to have more than one back up copy of Your data. If applicable law prohibits exclusion of liability for lost data, then Licensor will only be liable for the cost of the typical effort to recover the lost data from Your last available back up.

12.3. Limitation Period. Except as stated in this Section, all claims must be made within the period specified by applicable law. If the law allows the parties to specify a shorter period for bringing claims, or the law does not provide a time at all, then claims must be made within 18 months after the cause of action accrues.

## 13. Additional Terms.

13.1. Notices. The parties will provide all notices under this EULA in writing. Unless provided otherwise in an Order, You must provide notices to the local Dell entity in Your Order, or, if Your Order is not with a Dell entity, by e-mail to [Dell\\_Legal\\_Notices@dell.com](mailto:Dell_Legal_Notices@dell.com).

13.2. Waiver and Severability. Failure to enforce a provision of this EULA will not constitute a waiver of that or any other provision of this EULA. If a court of competent jurisdiction determines that any part of this EULA or document that incorporates this EULA by reference is unenforceable, that ruling will not affect the validity of all remaining parts.

13.3. Modifications. This EULA may only be modified in writing signed by both parties; provided, however, that Licensor may, in its sole discretion, update the Licensor Table, the OST Table, the UOM Terms and the Subscription Terms at any time. Any changes that Licensor makes to the Licensor Table, the OST Table, the UOM Terms or the Subscription Terms will only apply to Orders that occur after Licensor posts those changes online.

13.4. Governing Law and Jurisdiction. If You obtained the Software directly from Dell, then the governing law and jurisdiction provisions set forth in Your Order Terms shall apply to this EULA. Otherwise the following shall apply:

A. Subject to Section 13.4 D and 13.5, if You are domiciled in the United States or Canada: (1) this EULA and any Dispute is governed by the laws of the State of Texas (excluding the conflicts of law rules) and the federal laws of the United States; and (2) to the extent permitted by law, the state and federal courts located in Texas will have exclusive jurisdiction for any Dispute. Both parties agree to submit to the personal jurisdiction of the state and federal courts located within Travis or Williamson County, Texas, and agree to waive any and all objections to the exercise of jurisdiction over the parties by those courts and to venue in those courts.

B. Subject to Section 13.4 D, if You are domiciled outside of the United States or Canada: (1) this EULA and any Dispute is governed by the substantive laws in force in the country in which the Licensor is located (as indicated in the Licensor Table located at [www.dell.com/swlicensortable](http://www.dell.com/swlicensortable)), without regard to its conflict of law rules; and (2) the exclusive place of jurisdiction for any Dispute shall be in such country.

C. In any event, neither the U.N. Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act shall apply to this EULA or any Dispute.

D. If You are an individual consumer, this Section 13.4 does not deprive You of the protection afforded to You by the provisions of mandatory consumer protections laws that are applicable to You, nor does it prevent you from seeking remedies or enforcing your rights as a consumer under such laws.



13.5. **Dispute Resolution and Binding Individual (non-class) Arbitration.** This Section only applies if You are an individual consumer that resides in (or obtained the Software in) the United States or Canada. All Disputes shall be resolved exclusively and finally by binding individual arbitration. This means You and Licensor waive any right to litigate disputes in a court or before a jury and neither You nor Licensor shall be entitled to join, consolidate, or include any claims belonging to or alleged or arising from, by or on behalf of any third party to an arbitration brought hereunder, or to arbitrate any claim as a class action, class representative, class member, or in a private attorney general capacity. If You reside in (or obtained the Software in) the United States, the arbitration will be administered by the American Arbitration Association (AAA), or JAMS. If You reside in (or obtained the Software in) Canada, arbitration will be at ADR Chambers pursuant to the general ADR Chambers Rules for Arbitration located at [www.adrchambers.com](http://www.adrchambers.com). The arbitration shall be conducted in the English language. The arbitration panel shall have exclusive authority to resolve any arbitrability issues including any dispute over this EULA or this arbitration provision's scope, application, meaning and enforceability. The arbitration panel shall be empowered to grant whatever relief would be available in court, including without limitation preliminary relief, injunctive relief and specific performance. Any award of the arbitration panel shall be final and binding immediately when rendered, and judgment on the award may be entered in any court of competent jurisdiction. If any portion of this arbitration agreement is found unenforceable, the unenforceable portion shall be severed and the remaining arbitration terms shall be enforced (but in no event will there be a class arbitration). Consumer claimants (individuals whose transaction is intended for personal, family or household use) may elect to pursue their claims in small-claims court rather than arbitration. Licensor will be responsible for paying any individual consumer's arbitration/arbitrator fees. Notwithstanding the foregoing, Licensor may apply to any relevant government agency or any court of competent jurisdiction to preserve its rights under this EULA and to obtain any injunctive or preliminary relief, or any award of specific performance, to which it may be entitled, either against You or against a non-party; provided, however, that no such administrative or judicial authority shall have the right or power to render a judgment or award (or to enjoin the rendering of an arbitral award) for damages that may be due to or from either party under this EULA, which right and power shall be reserved exclusively to an arbitration panel proceeding in accordance herewith.

13.6. **Third Party Rights.** Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.7. **Entire Agreement.** You acknowledge that You have read this EULA, that You understand it, that You agree to be bound by its terms, and that this EULA, along with the Order Terms into which this EULA may be incorporated (as applicable), is the complete and exclusive statement of the agreement between You and Licensor regarding Your use of the Software. All content referenced in this EULA by hyperlink is incorporated into this EULA in its entirety and is available to You in hardcopy form upon Your request. The pre-printed terms of Your purchase order or any other document that is not issued or signed by Licensor or Dell do not apply to Software. You represent that You did not rely on any representations or statements that do not appear in this EULA when accepting this EULA.

EULA (rev. 23OCT2024)

ROW OOB file rev. 25OCT2024

DELLT\_DELLEULA\_10252024

## Amazon WorkSpaces Application License Agreement

THIS IS AN AGREEMENT BETWEEN YOU AND AWS MOBILE LLC (WITH ITS AFFILIATES, "AWS MOBILE" OR "WE") THAT GOVERNS YOUR USE OF THE AMAZON WORKSPACES APPLICATION FOR YOUR DEVICE (TOGETHER WITH ANY UPDATES AND ENHANCEMENTS TO IT, AND ACCOMPANYING DOCUMENTATION, THE "APPLICATION") THAT WE MAKE AVAILABLE TO YOU ON YOUR MOBILE, DESKTOP, OR OTHER SUPPORTED DEVICE (EACH, A "DEVICE"). IF YOU INSTALL OR USE THE APPLICATION, YOU WILL BE BOUND BY THIS AGREEMENT.

1. **Use of the Application.** We hereby grant you a personal, limited, non-exclusive, nontransferable, non-sublicenseable license to install and use the Application on your Device.
2. **Limitations.** You may not, and you will not encourage, assist or authorize any other person to: Incorporate any portion of the Application into your own programs or compile any portion of it in combination with your own programs. Sell, rent, lease, lend, loan, distribute, act as a service bureau, publicly communicate, transform, or sub-license the Application or otherwise assign any rights to the Application in whole or in part. Modify, alter, tamper with, repair, or otherwise create derivative works of the Application. Reverse engineer, disassemble, or decompile the Application or apply any other process or procedure to derive the source code of any software included in the Application. All rights granted to you are conditioned on your continued compliance with this Agreement, and will immediately and automatically terminate if you do not comply.
3. **Reservation of Rights.** You may not use the Application for any illegal purpose. The Application is the intellectual property of Amazon.com, Inc. or its affiliates, and its licensors. The structure, organization, and code of the Application are valuable trade secrets and confidential information of Amazon.com, Inc. or its affiliates. The Application is protected by law, including without limitation copyright laws and international treaty provisions. Except for the rights explicitly granted to you in this Agreement, all right, title and interest in the Application are reserved and retained by us and our licensors.

4. Updates. In order to keep the Application up-to-date, we may offer automatic or manual updates at any time and without notice to you. If we elect to provide maintenance or support of any kind, we may terminate that maintenance or support at any time without notice to you.
5. Termination. You may terminate this Agreement at any time by uninstalling or destroying all copies of the Application that are in your possession or control. In the case of termination, you must cease all use and destroy all copies of the Application. We may also terminate your right to use the Application at any time and if we do so, we may modify the Application to make it inoperable. Our failure to insist upon or enforce your strict compliance with this Agreement will not constitute a waiver of any of our rights.
6. Disclaimer of Warranties and Limitation of Liability. Use of the Application is at your sole risk. The Application is delivered "as is" with all faults and without warranty of any kind. To the extent not prohibited by law, no party will be liable to you for any incidental or consequential damages for breach of any express or implied warranty, breach of contract, negligence, strict liability, or any other legal theory related to the Application.
  - a. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT INSTALLATION AND USE OF, AND ANY OTHER ACCESS TO, THE APPLICATION IS AT YOUR SOLE RISK. THE APPLICATION IS DELIVERED TO YOU "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND AWS MOBILE, ITS LICENSORS AND DISTRIBUTORS, WIRELESS CARRIERS OVER WHOSE NETWORK THE APPLICATION IS DISTRIBUTED, AND EACH OF THEIR RESPECTIVE AFFILIATES AND SUPPLIERS (COLLECTIVELY, THE "RELEASED PARTIES") DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, QUIET ENJOYMENT, AND NON-INFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY A RELEASED PARTY OR AN AUTHORIZED REPRESENTATIVE OF A RELEASED PARTY WILL CREATE A WARRANTY. THE LAWS OF CERTAIN JURISDICTIONS DO NOT ALLOW THE DISCLAIMER OF IMPLIED WARRANTIES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS, OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS.
  - b. TO THE EXTENT NOT PROHIBITED BY LAW, NO RELEASED PARTY WILL BE LIABLE TO YOU FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY RELATED TO THE APPLICATION, INCLUDING WITHOUT LIMITATION ANY DAMAGES ARISING OUT OF LOSS OF PROFITS, REVENUE, DATA, OR USE OF THE APPLICATION, EVEN IF A RELEASED PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, ANY RELEASED PARTY'S AGGREGATE LIABILITY UNDER THE AGREEMENT WILL BE LIMITED TO \$50.00. THE LAWS OF CERTAIN JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS.
7. Indemnification. You are liable for and will defend, indemnify, and hold harmless the Released Parties and their officers, directors, agents, and employees, from and against any liability, loss, damage, cost, or expense (including reasonable attorneys' fees) arising out of your use of the Application, violation of this Agreement, violation of applicable law, or violation of any right of any person or entity, including without limitation intellectual property rights.
8. Export Regulations. You will comply with all export and re-export restrictions and regulations of the United States Department of Commerce and other United States and foreign agencies and authorities that may apply to the Application, and not to transfer, or encourage, assist, or authorize the transfer of the Application to a prohibited country or otherwise in violation of any applicable restrictions or regulations.
9. U.S. Government End Users. The Application is a "Commercial Item" as that term is defined in 48 C.F.R. § 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as the terms are used in 48 C.F.R. § 12.212 or 48 C.F.R. § 227.7202, as applicable. Consistent with these provisions, the Application is licensed to U.S. Government end users: (a) only as a Commercial Item; and (b) with only those rights as are granted to all other end users pursuant to these Terms of Use. Unpublished-rights are reserved under U.S. copyright laws.
10. Amendment. We may amend this Agreement at our sole discretion by posting the revised terms on the Amazon Web Services website (located at: <http://aws.amazon.com>) or within the Application. Your continued use of the Application after any amendment's effective date evidences your agreement to be bound by it.
11. Conflicts. The terms of this Agreement govern the Application and any updates or upgrades to the Application that we may provide that replace or supplement the original Application, unless the update or upgrade is accompanied by a separate license, in which case the terms of that license will govern.
12. Contact Information. For communications concerning this Agreement, please write to AWS Mobile LLC, Attn: Legal Department, 410 Terry Avenue North, Seattle, WA 98109-5210. The Application may include the WorkSpaces Streaming Protocol ("WSP") or software developed and owned by Teradici Corporation or its licensors ("PCoIP"). To determine whether the Application includes WSP or PCoIP, you should ask your Amazon WorkSpaces administrator, or look in the Support tab under About My WorkSpace after you successfully log in to the WorkSpace. The About My WorkSpace dialog box will identify WSP or PCoIP under Protocol. If the Application includes PCoIP, then Teradici Corporation and its licensors require that you agree to the following additional terms and conditions in connection with the use of PCoIP. BY SELECTING "AGREE" OR "I ACCEPT THE TERMS IN THE LICENSE AGREEMENT" AND/OR INSTALLING, ACTIVATING AND/OR USING THIS LICENSED PRODUCT (AS DEFINED BELOW), YOU OR THE ENTITY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THE LICENSE AGREEMENT WITH TERADICI CORPORATION ("TERADICI") CONSISTING OF THIS PARAGRAPH AND THE FOLLOWING TERMS (THIS "AGREEMENT") WITH RESPECT TO THE LICENSED PRODUCT. PROVISION OF THE

LICENSED PRODUCT IS CONDITIONED ON, AND LICENSEE'S INSTALLATION OR USE OF THE LICENSED PRODUCT SHALL CONSTITUTE, LICENSEE'S ASSENT TO THE TERMS OF THIS AGREEMENT OR OF SUCH EXISTING SEPARATE WRITTEN LICENSE AGREEMENT TO THE EXCLUSION OF ALL OTHER TERMS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO SUCH TERMS. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO THE FOREGOING, LICENSEE SHOULD NOT SELECT "AGREE" OR "I ACCEPT THE TERMS IN THE LICENSE AGREEMENT" AND/OR INSTALL, ACTIVATE AND/OR USE THE LICENSED PRODUCT. IF YOU CONTINUE WITH USE OR INSTALLATION, YOU ARE REPRESENTING AND WARRANTING THAT YOU ARE AUTHORIZED TO BIND LICENSEE.

1. **Grant of License and Restrictions.** Subject to the terms hereof, payment of any applicable fees, and any applicable user/use limitations [specified in this Agreement or by Amazon], Teradici grants Licensee a personal, non-sublicensable, non-transferable, nonexclusive, right to use a licensed product in object code form only ("Licensed Product"). For these purposes, "Licensed Product" shall include software (including firmware that may be loaded on, embedded in or otherwise included with a product purchased by you ("Purchased Product")), any updates to it and all Teradici and/or third-party proprietary documentation included with the software. Except for one copy solely for back-up purposes, Licensee may possess only the number of copies of any Licensed Product as has been expressly authorized by Amazon; Teradici retains ownership of the Licensed Product and all copies (including all intellectual property rights therein) and Licensee will maintain the copyright notice and any other notices that appear on the Licensed Product on any copies and any media. Licensee will not (and will not allow any third party to): (i) reverse engineer, decompile or attempt to discover any source code or underlying ideas or algorithms of any Licensed Product (except to the extent that applicable law prohibits reverse engineering restrictions), (ii) use the Licensed Product on or in connection with any client device not designated by Amazon (including client devices whose primary function is to deliver desktops and applications via remote display protocols (e.g., "thin" and "zero" clients), (iii) use the Licensed Product to connect to or interoperate with any non-Amazon or non-Teradici offering; (iv) provide, lease, lend, disclose, use for timesharing or service bureau purposes, or otherwise use or allow others to use for the benefit of any third party, any Licensed Product (except as expressly and specifically authorized by Teradici), (v) possess or use any Licensed Product, or allow the transfer, transmission, export, or re-export of any Licensed Product or portion thereof in violation of any export control laws or regulations administered by the U.S. Commerce Department, U.S. Treasury Department's Office of Foreign Assets Control, or any other government agency, (vi) disclose to any third party any benchmarking or comparative study involving any Licensed Product or (vii) modify any Licensed Product. Prior to disposing of any media or apparatus containing any part of the Licensed Product, Licensee shall completely destroy any Licensed Product contained therein. Further, a Licensed Product specifically licensed for evaluation purposes, without charge or for a nominal charge, will be deemed a free evaluation license and may be used for purposes of evaluation for a paid license only, and not for any productive use. Licensee acknowledges that Licensed Product may be distributed alongside or contain or use certain third party software ("Third Party Software"). THIRD PARTY SOFTWARE IS (IN ADDITION TO THE TERMS AND CONDITIONS OF THIS AGREEMENT), SUBJECT TO AND GOVERNED BY (AND LICENSEE AGREES TO, AND WILL INDEMNIFY TERADICI FOR NONCOMPLIANCE WITH) THE RESPECTIVE LICENSES FOR THE THIRD PARTY SOFTWARE AVAILABLE AT <http://www.teradici.com/docs/third-party-licenses.php>.
2. **Termination.** All licenses will terminate thirty days (immediately in the case of a breach of Section 1) after notice of any breach of this Agreement by Licensee that remains uncured at the end of such notice period. A license will also terminate upon the expiration of Licensee's right to use the AWS Services with which Licensee's use of the Licensed Product is authorized. Upon any termination, Licensee shall immediately cease all use of all affected Licensed Products and return or destroy all copies of all affected Licensed Products and all portions thereof and so certify to Teradici. Except as otherwise expressly provided herein, the terms hereof shall survive any termination. Termination is not an exclusive remedy and all other remedies will be available whether or not termination occurs.
3. **Confidentiality.**
  - a. **Definitions.**
    - i. "Confidential Information" means a Teradici's or Teradici's affiliates' non-public information (including copies, summaries, and extracts): (A) that is identified in writing as confidential at the time of disclosure, whether in printed, textual, graphic, or electronic form; or (B) that is disclosed in non-tangible form, identified as confidential at the time of disclosure, summarized in a writing labelled as "confidential", and delivered to Licensee or Licensee's affiliate (as applicable) within 15 days after disclosure. Confidential Information does not include information that:
      - A. is or becomes generally publicly available at or after the time of disclosure through no fault of either Licensee or Licensee's affiliate;
      - B. was known to Licensee or Licensee's affiliate (as applicable), free of any confidentiality obligations, before its disclosure by either Teradici or Teradici's affiliate;
      - C. becomes known to Licensee or Licensee's affiliate (as applicable), free of any confidentiality obligations, from a source other than either Teradici or Teradici's affiliate; or
      - D. is independently developed by either Licensee or Licensee's affiliate without use of Confidential Information.
    - ii. **No Use or Disclosure.** Licensee will only use Confidential Information for the purposes of this Agreement and will not reproduce, disseminate, or disclose Confidential Information to any person, except to its affiliates, employees and authorized representatives (i.e., temporary employees, consultants, and contractors) who need to know the Confidential Information for the purposes of this Agreement and are bound by confidentiality obligations at least as restrictive as those in this Section 3 (Confidentiality). Licensee will treat all Confidential Information with at least the same degree of care as it treats its own information of similar sensitivity, but never with less than reasonable care.

- iii. Required Disclosure. Licensee may disclose Confidential Information: (i) as approved in a writing signed by Teradici; (ii) as necessary to comply with any law or valid order of a court or other governmental body; or (iii) as necessary to establish the rights of either party, but only if, in the case of Section 3(c) (ii) and Section 3(c)(iii), Licensee (A) promptly notifies Teradici the particulars of the required disclosure; and (B) gives Teradici all assistance reasonably required by Teradici to enable Teradici to take available steps to prevent the disclosure or to ensure that disclosure occurs subject to an appropriate obligation of confidence.
- iv. Responsibility for Representatives and Affiliates. Licensee is responsible for ensuring that its employees, authorized representatives and affiliates fully comply with the obligations of the Licensee under this Section 3 (Confidentiality).
4. Limited Warranty and Disclaimer. ALL PRODUCTS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND FROM ANYONE INCLUDING TERADICI'S SUPPLIERS OR LICENSORS, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT. FURTHER, TERADICI DOES NOT WARRANT RESULTS OF USE OR THAT THE PRODUCTS ARE BUG FREE OR THAT THE PRODUCT'S USE WILL BE UNINTERRUPTED.
5. Limitation of Liability. NOTWITHSTANDING ANYTHING ELSE HEREIN OR OTHERWISE, AND EXCEPT FOR BODILY INJURY, NEITHER TERADICI NOR ANY TERADICI SUPPLIER OR LICENSOR SHALL BE LIABLE OR OBLIGATED WITH RESPECT TO THE SUBJECT MATTER HEREOF OR UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY (I) [FOR ANY AMOUNTS IN EXCESS IN THE AGGREGATE OF [TBD]] OR (II) FOR ANY COST OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY, SERVICES OR RIGHTS; (III) FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES (INCLUDING LOST PROFITS OR COST SAVINGS) EVEN IF LICENSEE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (IV) FOR INTERRUPTION OF USE OR LOSS OR CORRUPTION OF DATA; OR (V) FOR ANY MATTER BEYOND ITS REASONABLE CONTROL. THE LICENSED PRODUCT IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE WHERE THE FAILURE OF THE LICENSED PRODUCT COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SIGNIFICANT PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). USE OF THE LICENSED PRODUCT IN HIGH RISK ACTIVITIES IS NOT AUTHORIZED. THE PARTIES AGREE THAT THIS SECTION 5 REPRESENTS A REASONABLE ALLOCATION OF RISK AND THAT TERADICI WOULD NOT PROCEED IN THE ABSENCE OF SUCH ALLOCATION.
6. Miscellaneous. Neither this Agreement nor the licenses granted hereunder are assignable or transferable by Licensee (and any attempt to do so shall be void). A change of control (directly or indirectly) shall be defined as an assignment or transfer under this Agreement. Teradici may assign and transfer this Agreement and the licenses granted hereunder without restriction. The provisions hereof are for the benefit of the parties only and not for any other person or entity. Any notice, report, approval, authorization, agreement or consent to or by Teradici required or permitted hereunder shall be in writing addressed to: Teradici Corporation, Suite 101, 4621 Canada Way, Burnaby, BC V5G4X8, Canada. No failure or delay in exercising any right hereunder will operate as a waiver thereof, nor will any partial exercise of any right or power hereunder preclude further exercise. If any provision shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this arrangement shall otherwise remain in full force and effect and enforceable. This agreement shall be deemed to have been made in, and shall be construed pursuant to the laws of the State of California and the United States without regard to conflicts of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods or the Uniform Computer Information Transactions Act. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter hereof and any waivers or amendments shall be effective only if made in writing. The substantially prevailing party in any action to enforce this agreement will be entitled to recover its attorney's fees and costs in connection with such action. The Licensed Product (i) was developed at private expense and includes trade secrets and confidential information; (ii) is a commercial item consisting of commercial computer software and commercial computer software documentation regulated under FAR 52.227-14 and DFARS Section 227.7202 and shall not be deemed to be non-commercial computer software and/or non-commercial computer software documentation under any provision of DFARS; (iii) is NOT offered to US Government agencies under the commercial computer software license set forth at FAR 52.227-19. Consistent with 48 CFR 12.212 and 48 CFR 227.7202 as applicable, the Product is licensed to government end users solely as a commercial item and with only those rights as are granted to other end users under the terms of this Agreement. Technical data relating to commercial items shall be made available to the Government consistent with the requirements and limitations of FAR 52.227-14 or DFARS 252.227-7015, as applicable. The terms "commercial computer software," "commercial computer software documentation," "technical data relating to commercial items," shall have the meanings relating to each such term as are set forth in the aforementioned FAR and DFARS clauses, as applicable. All rights not expressly granted are expressly reserved by Teradici. Licensee is responsible for all acts and omissions of its affiliates or any person or entity whom Licensee is permitted under this Agreement to allow the use of or access to the Licensed Product. Nothing in this Agreement will be construed as creating an employer-employee relationship, a partnership, or a joint venture between the parties.

# VMWARE END USER LICENSE AGREEMENT

THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA") GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

BY DOWNLOADING, DEPLOYING, OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, DEPLOY, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO US OR THE VMWARE CHANNEL PARTNER FROM WHICH YOU ACQUIRED IT WITHIN THIRTY

(30) DAYS OF ITS ACQUISITION AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

**EVALUATION LICENSE.** If you license the Software for evaluation purposes (an "Evaluation License"), your use of the Software is only permitted for a period of thirty

(30) days (unless we specify otherwise), and you may not use the Software with production data. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS IS" without indemnification, support or warranty of any kind, express or implied.

## LICENSE GRANT

- **1. General License Grant.** We grant you a non-exclusive, non-transferable (except as set forth in Section 12.1 (Transfers; Assignment)) license to deploy the Software within the Territory and to use the Software and the Documentation during the term of the license, solely for your internal business operations, and subject to the provisions of the Product Guide. Unless otherwise set forth in the Order, licenses granted to you will be for use of object code only and will commence on Delivery.
- 2. Users and Third-Party Agents.** Under the License granted to you in Section 1.1 (General License Grant), you may permit your Users to use the Software, and you may permit Third-Party Agents to deploy and use the Software on your behalf for the sole purpose of delivering services to you. You will be responsible for your Users' and Third-Party Agents' compliance with this EULA, and any breach of this EULA by a User or Third-Party Agent will be deemed to be a breach by you.
- 3. Copying Permitted.** You may copy the Software and Documentation as necessary to deploy and use the number of copies licensed, but otherwise for archival purposes only.
- 4. Benchmarking.** You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or distribute the results of the studies to third parties if we have reviewed and approved of the methodology, assumptions, and other parameters of the study prior to publication and distribution. Please contact us at [benchmark@vmware.com](mailto:benchmark@vmware.com) to request review and approval.
- 5. Services for Affiliates.** You may use the Software to deliver IT services to your Affiliates, provided that those Affiliates may not directly use the Software.
- 6. Open Source Software.** Open Source Software is licensed to you under the OSS's own applicable license terms, which can be found in either the `open_source_licenses.txt` file accompanying the Software, the Documentation, or as applicable the corresponding Source Files (as defined below) for the OSS available at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html). These OSS license terms are consistent with the license granted in Section 1 (License Grant) and may contain additional rights benefiting you. The OSS license terms take precedence over this EULA to the extent that this EULA imposes greater restrictions on you than the applicable OSS license terms. To the extent the license for any Open Source Software requires us to make available to you the corresponding source code and/or modifications (the "**Source Files**"), you may obtain a copy of the applicable Source Files from our website at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html) or by sending a written request, with your name and address, to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you acquired the Software. **RESTRICTIONS; OWNERSHIP.**
- 7. License Restrictions.** Without our prior written consent, you must not, and must not allow any third party to: (a) use the Software in an application services provider, service bureau, hosted IT services, or similar capacity for third parties, except as specified in Section 1.5 (Services for Affiliates); (b) disclose to any third party the results of any benchmarking testing or comparative or competitive analyses of the Software done by you or on your behalf, except as specified in Section 1.4 (Benchmarking); (c) make available the Software in any form to any third parties, except as specified in Section 1.2 (Users and Third-Party Agents); (d) transfer or sublicense the Software or Documentation to an Affiliate or any third party, except as expressly permitted in Section 12.1 (Transfers; Assignment); (e) use the Software in conflict with the terms and restrictions of the Software's licensing model and other requirements specified in the Product Guide and/or the applicable Order; (f) except to the extent permitted by applicable mandatory law, modify, translate, enhance, or create derivative works from the Software, or reverse engineer, decompile, or otherwise attempt to derive source code from the Software, except as specified in Section 2.2 (Decompilation); (g) remove any copyright or other

proprietary notices on or in any copies of the Software; or (h) violate or circumvent any technological restrictions within the Software or specified in this EULA, such as via software or services.

8. **Decompilation.** Notwithstanding Section 2.1, you may decompile the Software to the extent the laws of the Territory give you the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, (a) you must first request that information from us, (b) you must provide all reasonably requested information to allow us to assess your claim, and (c) we may, in our discretion, provide that interoperability information to you, impose reasonable conditions (including a reasonable fee) on that use of the Software, or offer to provide alternatives to reduce any potential adverse impact on our proprietary rights in the Software.
9. **Ownership.** The Software and Documentation (including all copies and portions), all improvements, enhancements, modifications and derivative works of the Software or Documentation, and all Intellectual Property Rights in the Software and Documentation, are and will remain the sole and exclusive property of VMware and its licensors. Your rights to deploy and use the Software and Documentation are limited to those expressly granted in this EULA and any applicable Order. No other rights are implied with respect to the Software, Documentation, or any related Intellectual Property Rights. You are not authorized to use (and must not permit any third party to use) the Software or Documentation except as expressly authorized by this EULA or the applicable Order. We reserve all rights not expressly granted to you. We do not transfer any ownership rights in any Software or Documentation.
10. **Guest Operating Systems.** Some Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that you are responsible for obtaining and complying with any licenses necessary to operate any third-party software.
1. **ORDER.** Your Order is subject to this EULA. No Orders are binding on us until we accept them. Orders for Software are deemed accepted upon Delivery of the Software included in the Order. Purchase orders issued to us do not have to be signed by you to be valid and enforceable. All Orders are non-refundable and non-cancellable except as expressly provided in this EULA. Any refunds to which you are entitled under this EULA will be remitted to you or to the VMware channel partner from which you purchased your Software license.
2. **RECORDS AND AUDIT.** You must maintain accurate records of your use of the Software sufficient to show compliance with the terms of this EULA. We have the right to audit those records and your use of the Software to confirm compliance with the terms of this EULA. That audit is subject to reasonable prior notice and will not unreasonably interfere with your business activities. We may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. You must reasonably cooperate with us and any third-party auditor and you must, without prejudice to our other rights, address any non-compliance identified by the audit by paying additional fees. You must reimburse us for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the Software fees payable by you for the period audited, or that you have materially failed to maintain accurate records of Software use.
3. **SUPPORT SERVICES.** Support and subscription services for the Software ("**Support Services**") are provided pursuant to the Support Services Terms and are not subject to this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software unless you separately purchase Support Services or they are included with your purchase of a license to the Software as provided in the Product Guide. **WARRANTIES.**
  - a. **Software Warranty: Duration and Remedy.** We warrant that the Software will, for a period of ninety (90) days following notice of availability for electronic download or delivery ("**Warranty Period**"), substantially conform to the applicable Documentation, provided that the Software: (a) has been properly installed and used at all times in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than us or our authorized representative. We will, at our own expense and as our sole obligation and your exclusive remedy for any breach of this warranty, either replace the Software or correct any reproducible error in the Software reported by you in writing during the Warranty Period. If we determine that we are unable to correct the error or replace the Software, we will refund the fees paid for that Software, and the License for that Software will terminate.
  - b. **Disclaimer of Warranty.** OTHER THAN THE LIMITED WARRANTY IN SECTION 6.1, TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE, FOR OURSELVES AND ON BEHALF OF OUR SUPPLIERS, DISCLAIM ALL WARRANTIES WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE, RELATING TO THE SOFTWARE AND DOCUMENTATION. NEITHER WE NOR OUR SUPPLIERS WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED, THAT IT WILL BE FREE FROM DEFECTS OR ERRORS, OR THAT IT WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS. **INTELLECTUAL PROPERTY INDEMNIFICATION.**
  - c. **Defense and Indemnification.** Subject to the remainder of this Section 7, we will: (a) defend you against any Infringement Claim; and (b) indemnify you from all fines, damages, and costs finally awarded against you by a court of competent jurisdiction or a government agency, or agreed to in a settlement, with regard to any Infringement Claim. These obligations are applicable only if you: (i) provide us with notice of the Infringement Claim within a reasonable period after learning of the claim (provided that any delay in providing the notice will relieve us of our indemnification obligations only to the extent that the delay prejudices us); (ii) allow us sole control over the defense and settlement of the Infringement Claim; and (iii) reasonably cooperate in response to our requests for assistance with regard to the Infringement Claim. We will not, without your prior written consent, which may not be unreasonably withheld, conditioned, or delayed, enter into any settlement of any Infringement Claim that obligates you to admit any liability or to pay any unreimbursed amounts to the claimant. You may not settle or compromise any Infringement Claim without our prior written consent.

- d. **Remedies.** If the Software becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will, at our option and expense: (a) procure the rights necessary for you to keep using the Software; or (b) modify or replace the Software to make it non-infringing; or (c) terminate the License to the affected Software and discontinue the related Support Services, and, upon your certified deletion of the affected Software, refund: (i) for a Perpetual License, the fees paid for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date of Delivery of the Software and any unused, prepaid fees for Support Services, or (ii) for Subscription Software, any prepaid fees, prorated for the remaining portion of the then-current Subscription Term.
- e. **Exclusions.** We will have no obligation under this Section 7 or otherwise with respect to any Infringement Claim based on: (a) combination of the Software with non-VMware products or content; (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer version would have avoided the infringement; (d) any modification to the Software other than those made by us or with our express written approval; (e) any claim that relates to open source software or freeware technology or any derivative or other adaptations thereof that is not embedded by us into the Software; or (f) any Software provided on a no charge, beta, or evaluation basis.
- f. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS SECTION 7 STATES YOUR SOLE AND EXCLUSIVE REMEDY AND OUR ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS. **LIMITATION OF LIABILITY.**
- g. **Disclaimer.** TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL WE BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF CONTENT OR DATA FOR ANY REASON (INCLUDING POWER OUTAGES, SYSTEM FAILURES, OR OTHER INTERRUPTIONS), LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. THIS LIMITATION WILL APPLY REGARDLESS OF WHETHER A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE FOREGOING LIMITATION MAY NOT APPLY.
- h. **Cap on Monetary Liability.** OUR LIABILITY FOR ANY CLAIM UNDER THIS EULA WILL NOT EXCEED THE GREATER OF THE LICENSE FEES YOU PAID FOR THE SOFTWARE GIVING RISE TO THE CLAIM OR \$5000.
- i. **Exclusions.** THE LIMITATION OF LIABILITY IN SECTIONS 8.1 AND 8.2 WILL NOT APPLY TO (i) OUR INDEMNIFICATION OBLIGATIONS UNDER SECTION 7 OF THIS EULA OR (ii) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY LAW.
- j. **Further Limitations.** Our suppliers have no liability of any kind under this EULA. You may not bring a claim directly against any of them under this EULA. Our liability with respect to any third-party software embedded in the Software is subject to this Section 8. You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises. **TERMINATION.**
- k. **EULA Term.** The term of this EULA begins on Delivery of the Software and continues until this EULA is terminated in accordance with this Section 9.
- l. **Termination for Cause.** We may terminate this EULA effective immediately upon written notice to you if: (a) any payment due under this EULA is not received within ten (10) days after receiving our written notice that payment is past due; (b) you materially breach any other provision of this EULA and fail to cure within thirty (30) days after receipt of our written notice of the breach; (c) you materially breach any provision of this EULA in a manner that cannot be cured; or (d) you terminate or suspend your business.
- m. **Termination for Insolvency.** We may terminate this EULA effective immediately upon written notice to you if you become insolvent, admit in writing your inability to pay your debts as they mature, make an assignment for the benefit of creditors, become subject to control of a trustee, receiver or similar authority, or become subject to any bankruptcy or insolvency proceeding.
- n. **Effect of Termination.** Upon termination of this EULA: (a) all Licenses to the Software granted to you under this EULA will immediately end; (b) you must stop all use of the Software and return to us or certify destruction of the Software and License Keys (including copies), and (c) you must return or, if we request, destroy, any of our or our suppliers' Confidential Information in your possession or under your control (other than information that must be retained pursuant to law). Any provision that, by its nature and context is intended to survive termination or expiration of the EULA, will survive, including Sections 1.6 (Open Source Software), 2 (Restrictions; Ownership), 4 (Records and Audit), 6.2 (Software Disclaimer of Warranty), 8 (Limitation of Liability), 9 (Termination), 10 (Confidential Information), 12 (General), 13 (Definitions), and 14 (Terms Applicable to U.S. Federal End Users). Except as otherwise expressly provided in this EULA or as required by applicable law or regulation, termination of this EULA will not entitle you to any refunds, credits, or exchanges. **CONFIDENTIAL INFORMATION.**
- o. **Protection.** Either party may use Confidential Information of the other party disclosed to it in connection with this EULA to exercise its rights and perform its obligations under this EULA or as otherwise permitted by this EULA. The Recipient will disclose the Discloser's Confidential Information only to the Recipient's employees or contractors who have a need to know the Confidential Information for purposes of this EULA and who are under a duty of confidentiality no less restrictive than as specified in this Section 10. Recipient will protect the Discloser's Confidential Information from unauthorized use, access, or disclosure in the same manner as the Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

- p. **Exceptions.** The Recipient's obligations under Section 10.1 with respect to any of the Discloser's Confidential Information will terminate if the Recipient can demonstrate that the information: (a) was already rightfully known to the Recipient at the time of disclosure by the Discloser without any obligation of confidentiality; (b) was disclosed to the Recipient by a third party who had the right to make that disclosure without any confidentiality restrictions; (c) is, or through no fault of the Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to or use of Discloser's Confidential Information. In addition, the Recipient will be allowed to disclose Confidential Information to the extent that disclosure is required by law or by order of a court or similar judicial or administrative body of competent jurisdiction, provided that the Recipient notifies the Discloser of the required disclosure promptly and in writing and cooperates with the Discloser, at the Discloser's request and expense, in any lawful action to contest or limit the scope of the required disclosure.
- q. **Injunctive Relief.** Nothing in this EULA limits either party's ability to seek equitable relief.
4. **ACCOUNT, OPERATIONS AND USAGE DATA.** We collect your contact information and information about your purchase to manage your account and fulfill your Orders. We also process (a) information necessary to facilitate the delivery of the Software, including verifying compliance with the terms of this EULA, invoicing, and providing Support Services, and (b) Software configuration, performance, and usage data for the purposes of improving VMware products and services and user experience, and other analytics purposes as set forth in the Product Guide. To the extent any of that data includes information which identifies an individual, we will process that information in accordance with VMware's Products & Services Privacy Notice available at <https://www.vmware.com/help/privacy.html>. **GENERAL.**
- a. **Transfers; Assignment.** Except to the extent transfer may not legally be restricted or as permitted by our transfer and assignment policies and in all cases following the process set forth at [www.vmware.com/support/policies/licensingpolicies.html](http://www.vmware.com/support/policies/licensingpolicies.html), you must not assign this EULA, any Order, or any right or obligation pursuant to this EULA, or delegate any performance under this EULA, without our prior written consent, which consent will not be unreasonably withheld, conditioned, or delayed. Any other attempted assignment or transfer by you will be void. We may use our Affiliates or other suppliers to provide services to you, provided that we remain responsible to you for the performance of the services.
- b. **Notices.** Any notice by us to you under this EULA will be given: (a) by email to the email address associated with your account, if you have subscribed to this method of receiving notices; or (b) by posting in the VMware customer portal. You must direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.
- c. **Waiver.** Waiver of a breach of any provision of this EULA will not constitute a waiver of any later breach of that provision, or waiver of a breach of any other provision.
- d. **Severability.** If any part of this EULA is held to be invalid or unenforceable, all remaining provisions will remain in force to the extent feasible to effectuate the intent of the parties.
- e. **Compliance with Laws.** Each party must comply with all laws applicable to the actions contemplated by this EULA.
- f. **Export Control; Government Regulations.** You acknowledge that the Software is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and Documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to Defense Federal Acquisition Regulation Supplement ("DFARS") Section 227.7202 and Federal Acquisition Regulation ("FAR") Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and Documentation by or for the U.S. Federal Government shall be governed solely by the terms and conditions of this EULA.
- g. **Construction.** The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word "including" means "including but not limited to".
- h. **Language.** This EULA is in English, and the English language version governs any conflict with a translation into any other language.
- i. **Governing Law.** If your billing address is in the United States, this EULA is governed by the laws of the State of California and the federal laws of the United States. If your billing address is outside the United States, this EULA is governed by the laws of Ireland. Conflict of law rules are expressly disclaimed. The U.N. Convention on Contracts for the International Sale of Goods does not apply.
- j. **Third-Party Rights.** Other than as expressly provided in this EULA, this EULA does not create any rights for any person who is not a party to it, and only persons who are parties to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.
- k. **Order of Precedence.** In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following descending order of precedence applies unless otherwise set forth in an enterprise license agreement: (a) the Product Guide, (b) this EULA and (c) the Order. This EULA supersedes any conflicting or additional terms and conditions of any purchase order, acknowledgement or confirmation, or other document issued by you for or regarding the Software.



- l. **Entire Agreement.** This EULA, together with all accepted Orders and the Product Guide, contains the entire agreement of the parties with respect to the subject matter of this EULA and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding its subject matter. This EULA may be amended only in a writing signed by authorized representatives of both parties. **DEFINITIONS.**
- m. **"Affiliate"** means, with respect to a party at a given time, an entity that is directly or indirectly controlled by, is under common control with, or controls that party, where "control" means an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests outstanding of that entity.
- n. **"Confidential Information"** means information or materials provided by one party ("**Discloser**") to the other party ("**Recipient**") which is in tangible form and labelled "confidential" or the like, or information which a reasonable person knew or should have known to be confidential. The following information is considered our Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding our pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software.
- o. **"Delivery"** means either delivery of the physical media (if applicable) or the date you are notified of availability for electronic download.
- p. **"Documentation"** means that documentation that we generally provide with the Software, as revised by us from time to time, and which may include end user manuals, operation instructions, installation guides, release notes, and on-line help files regarding the use of the Software.
- q. **"Guest Operating Systems"** means instances of third-party operating systems licensed by you, installed in a Virtual Machine, and run using the Software.
- r. **"Infringement Claim"** means any claim by a third party that the Software infringes any patent, trademark or copyright of that third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of your actions) under the laws of: (a) the United States; (b) Canada; (c) the European Economic Area; (d) the United Kingdom; (e) Australia; (f) New Zealand; (g) Japan; or (h) the People's Republic of China, to the extent that those countries are part of the Territory for the License.
- s. **"Intellectual Property Rights"** means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights, and all other proprietary rights, whether registered or unregistered.
- t. **"License"** means a license granted under Section 1.1 (General License Grant).
- u. **"License Key"** means a serial number that enables you to activate the Software.
- v. **"License Term"** means the duration of a License as specified in the Order.
- w. **"Open Source Software"** or **"OSS"** means software components embedded in the Software and provided under separate license terms, which can be found either in the open\_source\_licenses.txt file (or similar file) provided within the Software or at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html).
- x. **"Order"** means a purchase order, enterprise license agreement, or other ordering document for Software governed by this EULA, issued by you to us or to your VMware channel partner and is accepted by us as set forth in Section 3 (Order).
- y. **"Perpetual License"** means a License to the Software with a perpetual term.
- z. **"Product Guide"** means the current version of the VMware Product Guide at the time of your Order, which can be found through links at [www.vmware.com/download/eula](http://www.vmware.com/download/eula).
- aa. **"Support Services Terms"** means our then-current support policies, copies of which are posted at [www.vmware.com/support/policies](http://www.vmware.com/support/policies).
- ab. **"Software"** means the VMware computer programs listed on our commercial price list to which you acquire a license under an Order, together with any related software code we provide pursuant to a support and subscription service contract and that is not subject to a separate license agreement.
- ac. **"Subscription Software"** means Software that is licensed for a specific term ("**Subscription Term**").
- ad. **"Territory"** means the country or countries in which you have been invoiced, except as otherwise provided in the Product Guide. If the Territory for your Software includes any European Economic Area member states or the United Kingdom, you may deploy that Software throughout the European Economic Area and the United Kingdom.
- ae. **"Third-Party Agent"** means a third party delivering information technology services to you pursuant to a contract with you.
- af. **"U.S. Federal End User"** means any of the following agencies or establishments of the U.S. Federal Government: (a) executive departments as defined by 5 U.S.C. 101, (b) military departments as defined by 5 U.S.C. 102, (c) government corporations as defined by 5 U.S.C. 103, (d) independent establishments as defined by 5 U.S.C. 104, and (e) any establishment in the legislative or judicial branch of the U.S. Federal Government (except the Senate, the House of Representatives, the Architect of the Capitol, and any activities under the Architect's direction).
- ag. **"User"** means an employee, contractor, or Third-Party Agent that you have authorized to use the Software as permitted under this EULA.
- ah. **"Virtual Machine"** means a software container that can run its own operating system and execute applications like a physical machine.

- ai. **"VMware"**, **"We"**, or **"Us"** means VMware, Inc., a Delaware corporation, if the billing address for your Order is in the United States, or VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your Order is outside the United States.
  - aj. **"You"** means you individually or the legal entity that you represent. If you are entering into the EULA for an entity, you represent that you have the authority to bind that entity.
- 5. TERMS APPLICABLE TO U.S. FEDERAL END USERS.** If you are a U.S. Federal End User, the following terms and conditions supersede or modify the referenced provisions of this EULA.
- a. Replace the second paragraph of the preamble with the following: BY PURCHASING THE SOFTWARE UNDER A CONTRACT OR ORDER THAT INCORPORATES THIS EULA, YOU (THE U.S. FEDERAL END USER) AGREE TO BE BOUND BY THE TERMS OF THIS EULA.
  - b. Replace the first sentence of Section 1.1 ("General License Grant") with the following: "We grant you a non-exclusive, non-transferable (except as set forth in Section 12.1 (Transfers; Assignment)), commercial item license to deploy the Software within the Territory and to use the Software and the Documentation during the term of the license, solely for your internal business operations, and subject to the provisions of the Product Guide."
  - c. Replace Section 1.5 ("Services for Affiliates") with "Reserved."
  - d. Replace subsection (a) in the first sentence of Section 2.1 ("License Restrictions") with the following: (a) use the Software in an application services provider, service bureau, hosted IT services, or similar capacity for third parties;
  - e. Replace Section 3 ("Order") with the following: "Your Order is subject to this EULA. No Orders are binding on us until we accept them, and all Orders must expressly incorporate this EULA. Orders for Software are deemed accepted upon Delivery of the Software included in the Order. Purchase orders issued to us do not have to be signed by you to be valid and enforceable unless required by applicable law. All Orders are non-refundable and non- cancellable except as expressly provided in this EULA. Any refunds to which you are entitled under this EULA will be remitted to you or to the VMware channel partner from which you purchased your Software license."
  - f. Replace Section 4 ("Records and Audit") with the following: "You must maintain accurate records of your use of the Software sufficient to show compliance with the terms of this EULA. We have the right to audit those records and your use of the Software, at our own expense, to confirm compliance with the terms of this EULA. That audit is subject to reasonable prior notice and will not unreasonably interfere with your business activities. We may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. Neither we nor any third-party auditor shall have physical access to your computing devices in connection with any such audit without your prior written consent. You must reasonably cooperate with us and any third-party auditor. We reserve the right to seek recovery of any underpayments revealed by the audit in accordance with 41 U.S.C. chapter 71 (Contract Disputes) and FAR 52.233-1 (Disputes) or other applicable agency supplement. No payment obligation shall arise on your behalf until the conclusion of the dispute process. If an audit necessitates access to classified information, as that term is defined in the National Industrial Security Program Operating Manual (NISPOM), then the audit will be conducted by auditor(s) possessing a personal security clearance as defined in the NISPOM ("PCL") at the appropriate level. In those cases, VMware and any third-party auditor will disclose Classified Information only to person(s) who both possess a PCL and have a need to know."
  - g. Replace Section 7.1 ("Defense and Indemnification") with the following: "Subject to the remainder of this Section 7 and 28 U.S.C. 516, we will (a) defend you against an Infringement Claim; and (b) indemnify you from costs and damages finally awarded against you by a court of competent jurisdiction or a government agency or agreed to in a settlement approved by us. These obligations are applicable only if you: (i) provide us with notice of any Infringement Claim within a reasonable period after learning of the claim (provided that any delay in providing the notice will relieve us of our indemnification obligations only to the extent that the delay prejudices us); (ii) allow us the opportunity to participate in the claim's defense and settlement as provided in applicable laws, rules, or regulations; and (iii) reasonably cooperate in response to our requests for assistance with regard to the Infringement Claim. You must make every effort to permit us to participate fully in the defense or settlement of any Infringement Claim; however, we acknowledge that such participation will be under the control of the U.S. Department of Justice.
  - h. Replace Section 7.2 ("Remedies") with the following: If the Software becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will, at our option and expense: (a) procure the rights necessary for you to keep using the Software; or (b) modify or replace the Software to make it non-infringing. If we determine that the foregoing alternatives are not reasonably available, then you agree to terminate the License to the affected Software and discontinue the related Support Services upon our written request, and, upon your certified deletion of the affected Software, we will refund: (i) for a Perpetual License, the fees paid for the License to the affected Software, less straight- line depreciation over a three (3) year useful life beginning on the date of Delivery of the Software and any unused, prepaid fees for Support Services, or (ii) for Subscription Software, any prepaid fees, prorated for the remaining portion of the then-current Subscription Term. Nothing in this Section 7.2 (Remedies) will limit our obligations under Section 7.1 (Defense and Indemnification), provided that you replace the allegedly infringing Software upon our making alternate Software available to you, or that you discontinue using the allegedly infringing Software upon receiving VMware's written request to terminate the affected License. The foregoing is subject to the U.S. Federal Government's right to require continued use of the Software pursuant to 28 U.S.C. 1498. In the event of such continued use, you agree to notify us in writing and undertake at your expense the defense of any Infringement Claim against you, and we shall have no further indemnification obligation; however, we may participate at our own expense in the defense of any Infringement Claim if the claim is against us.

- i. Replace the last sentence of Section 8.4 (“Further Limitations”) with the following: You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises or such longer period as is mandated by 41 U.S.C. chapter 71 (Contract Disputes). Nothing in this Section 8 will impair the U.S. Federal Government’s right to recover for fraud or crimes arising out of this EULA as permitted under any applicable federal fraud statute, including the False Claims Act (31 U.S.C. 3729-3733).
- j. Add the following to the beginning of Section 9.2 (“Termination for Cause”): Subject to, and to the extent not prohibited by, 41 U.S.C. chapter 71 (Contract Disputes) and FAR 52.233-1 (Disputes),
- k. Replace Section 9.3 (“Termination for Insolvency”) with the following: **9.3. Termination by You.** You may terminate this EULA in accordance with FAR 52.212-4(l) or FAR 52.212-4(m), if applicable.”
- l. Replace Section 12.1 (“Transfers; Assignment”) with the following: Except to the extent transfer may not legally be restricted or as permitted by our transfer and assignment policies and in all cases following the process set forth at [www.vmware.com/support/policies/licensingpolicies.html](http://www.vmware.com/support/policies/licensingpolicies.html), you must not assign this EULA, any Order, or any right or obligation pursuant to this EULA, or delegate any performance under this EULA, without our prior written consent, which consent will not be unreasonably withheld, conditioned, or delayed. We may assign our right to receive payment in accordance with the Assignment of Claims Act (31 U.S.C. 3727) and FAR 52.212-4(b), and we may assign this EULA to the extent not prohibited by the Anti- Assignment Act (41 U.S.C. 15). Subject to the requirements of FAR 42.12 (Novation and Change-of-Name Agreements), you shall recognize our successor in interest following a transfer of our assets or a change in our name. Any other attempted assignment or transfer by either party will be void. Subject to the foregoing, this EULA will be binding upon and will inure to the benefit of the parties and their respective successors and assigns. We may use our affiliates or other suppliers to provide services to you, provided that we remain responsible to you for the performance of the services.”
- m. Replace Section 12.9 (“Governing Law”) with the following: This EULA is governed by the applicable federal laws of the United States. The U.N. Convention on Contracts for the International Sale of Goods does not apply.
- n. Add the following to the end of Section 12.10 (“Third-Party Rights”): Notwithstanding the foregoing, for any Orders placed with a VMware channel partner, the VMware channel partner may bring a claim to enforce the terms of this EULA at our request and on our behalf.
- o. Replace Section 12.11 (“Order of Precedence”) with the following: **“2.11. Product Guide.** The Product Guide is incorporated by reference in this EULA. To the extent that any terms and conditions in this EULA or in the Product Guide are inconsistent with applicable federal law, they shall be deemed deleted and unenforceable as applied to your Order. In the event of conflict or inconsistency among the Product Guide and this EULA, the Product Guide shall take precedence unless otherwise provided in an enterprise license agreement. This EULA supersedes any conflicting or additional license terms contained in any purchase order, acknowledgement or confirmation, or other document issued by you for or regarding the Software.”
- p. Replace Section 12.12 (“Entire Agreement”) with the following: “This EULA and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding its subject matter. This EULA may be amended only in writing signed by authorized representatives of both parties.”
- q. Replace Section 13.1 (“Affiliate”) with “Reserved.”
- r. Replace Section 13.12 (“Order”) with the following: **“‘Order’** means a purchase order, enterprise license agreement, or other ordering document issued by you to us or to your VMware channel partner that references and incorporates this EULA and is accepted by us as set forth in Section 3 (Order).”
- s. Replace Section 13.15 (“Support Services Terms”) with the following: **“‘Support Services Terms’** means our then-current support policies, copies of which are posted at [www.vmware.com/support/policies](http://www.vmware.com/support/policies), subject to FAR 52.212-4(u) and General Services Acquisition Manual (“GSAM”) 552.232-78 (Commercial Supplier Agreements— Unenforceable Clauses).”
- t. Replace Section 13.18 (“Territory”) with the following: **“‘Territory’** means the United States of America, including U.S. Federal Government Facilities located outside of the United States of America, except as otherwise provided in the Product Guide. For purposes of this section, “U.S. Federal Government Facilities” means buildings that are both 100% owned and controlled by the U.S. Federal Government and includes land, bases, installations, vessels, craft, and ships that are both 100% owned and controlled by the U.S. Federal Government. In the foregoing sentence, “owned” also includes leased throughout the entire term of the Order.”
- u. Replace Section 13.23 (“VMware,” “We,” or “Us”) with the following:  
**“‘VMware,’ ‘We,’ or ‘Us’** means VMware, Inc., a Delaware corporation.”

# Cisco General Terms

## 1. Scope and applicability

1.1 These terms (the “General Terms”) govern Your access to, and use of, Cisco Offers and incorporate any Supplemental Terms and Offer Descriptions applicable to Your Order. Capitalized terms are defined in section 14 (Definitions).

1.2 You agree to these terms by accessing or using a Cisco Offer, finalizing Your Order or through Your express agreement, whichever happens first. These terms apply independently of any contract You may have with a Cisco Partner.

## 2. Use Rights

2.1 License and right to use. Cisco grants You, for Your direct benefit, a non-exclusive:

- (a) license to use Software and Cisco Content; and
- (b) right to use Subscription Offers, including Cloud Services,

in accordance with Your Order or as otherwise agreed in writing (collectively, the “Use Rights”). Your Use Rights are non-transferable (except Software as permitted under the Transfer Policies).

2.2 Limits on usage. You may not:

- (a) transfer, sell, sublicense, monetize or provide the functionality of any Cisco Offer to any third party, except as authorized by Cisco;
- (b) use the Software on second hand or refurbished Cisco devices or use Software licensed for a specific device on a different device unless authorized by Cisco or permitted under the Transfer Policies;
- (c) remove, change, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks from any Cisco Offer;
- (d) reverse engineer, decompile, decrypt, disassemble, modify, or make derivative works of Cisco Offers; or
- (e) use Cisco Content other than as reasonably needed to exercise Your Use Rights.

2.3 Acceptable use. You will ensure Your access or use of Software or Subscription Offers does not:

- (a) violate applicable laws or the rights of any third party; or
- (b) impede or interfere with the security, stability, availability or performance of any Cloud Service, or any other network or service (e.g., denial-of-service attacks, penetration testing or distribution of malware).

2.4 Suspension. Cisco may suspend Your access to Software or Subscription Offers if it reasonably believes that You or an Authorized User have materially breached sections 2.2 (Limits on usage) or 2.3 (Acceptable use).

2.5 Use by third parties. If You permit Authorized Users to access Cisco Offers on Your behalf:

- (a) You will make sure all Authorized Users follow these terms; and
- (b) You are liable for any breach of these terms by an Authorized User.

2.6 Interoperability requirements. If required by law, Cisco will promptly provide the information You request to achieve interoperability between applicable Cisco Offers and another independently created program on terms that reasonably protect Cisco’s proprietary interests.

2.7 Use with third party products. Cisco does not support or guarantee integration with third party technologies or services unless they are included as part of a Cisco Offer or agreed in writing.

2.8 Changes to Subscription Offers. Cisco may change its Subscription Offers, typically to enhance them or add features. These changes will not materially reduce the core functionality of the affected Subscription Offers during the Use Term.

2.9 Maintaining Subscription Offers. Cisco may occasionally perform maintenance of its Subscription Offers which may disrupt the performance or availability of affected Subscription Offers. Cisco will provide advanced notice of planned maintenance when reasonably possible. If Cisco performs emergency maintenance without notice, it will take reasonable steps to reduce any disruption of affected Subscription Offers.

2.10 Open-source technology. Separate license terms apply to third party open-source technology used in Cisco Offers. Open-source terms are found at [Cisco's Open Source](#) webpage. As long as You use Cisco Offers according to these General Terms, Cisco’s use of open-source technology in Cisco Offers will not impede Your exercise of Use Rights or cause Your software to become subject to an open-source license.

## 3. Free trials

3.1 Accessing Free Trials. Your Approved Source may let You access or use Cisco Offers on a trial, evaluation, beta or other free-of-charge basis ("Free Trial"). You may only access or use the Free Trial for the period specified ("Free Trial Period") and under any additional terms specified by Your Approved Source in writing. If no Free Trial Period is specified, You may only access or use the Free Trial for 60 days after the Free Trial is available to You. Free Trials may not come with support and may be incomplete or have errors. Unless agreed in writing by Cisco, You will not use the Free Trial in a production environment.

3.2 Ending Free Trials. At the end of a Free Trial, You will promptly Return the Cisco Offers as described in the Free Trial terms. Your Approved Source may change or terminate a Free Trial at its discretion with reasonable notice.

3.3 Continued use and disclaimer.

(a) If You continue accessing a Cisco Offer after a Free Trial Period or fail to Return a Cisco Offer, You will pay any applicable fees reasonably charged by Your Approved Source.

(b) Unless agreed by Cisco in writing or required by law, Free Trials are provided "AS-IS" without any express or implied warranties.

## 4. End of life

4.1 Notification. Cisco may end the life of Cisco Offers by providing notice at the [End-of-Sale and End-of-Life Products](#) webpage.

4.2 Pre-paid Cloud Service. If Your Approved Source is prepaid a fee for Your use of a Cloud Service that is end of life before Your then-current Use Term ends, Cisco will either (a) provide You with a generally available alternative offer, or (b) if Cisco cannot reasonably provide an alternative offer, it will credit the unused balance of fees paid for the relevant Cloud Service to Your Approved Source or You (if Cisco is the Approved Source) once You Return the Cloud Service.

4.3 Credit. Credits issued under section 4.2 (Pre-paid Cloud Service) are calculated from the last date the applicable Cloud Service is available to the end of the applicable Use Term and may be applied only towards the future purchase of Cisco Offers.

## 5. Paying Your Approved Source

You will pay Your Approved Source all amounts due under Your Orders, including fees for additional consumption of a Subscription Offer or under a Buying Program.

## 6. Confidentiality

6.1 General obligation. A recipient of Confidential Information will protect that Confidential Information using the same standard of care it uses to protect its own confidential information of a similar nature, but no less than a reasonable standard of care. This section 6 (Confidentiality) will not apply to information which:

- (a) is known by the recipient without confidentiality obligations;
- (b) is or has become public knowledge through no fault of the recipient; or
- (c) is independently developed by, or for, the recipient.

6.2 Permitted recipients. A recipient of Confidential Information will not disclose Confidential Information to any third party, except to its employees, Affiliates and contractors who need to know. The recipient is liable for a breach of this section 6 by its permitted recipients and must ensure each of those permitted recipients have written confidentiality obligations at least as restrictive as the recipient's obligations under these terms.

6.3 Required disclosures. The recipient may reveal Confidential Information if required by law (including under a court order) but only after it notifies the discloser in writing (if legally permissible). A recipient will reasonably cooperate with a discloser's reasonably requested protective actions, at the discloser's expense.

6.4 Returning, destroying and retaining Confidential Information. The recipient will return, delete or destroy all Confidential Information and confirm in writing it has done so within 30 days of the discloser's written request unless retention is required by law or Confidential Information has been stored in a backup system in the ordinary course of business. Retained Confidential Information will continue to be subject to this section 6 for five years, or until the Confidential Information is no longer a trade secret under applicable law.

## 7. Privacy and security

7.1 Cisco respects Your Data and will access and use Data in accordance with the Data Briefs.

7.2 In addition, if Cisco processes Personal Data or Customer Content, Cisco will process such data according to:

- (a) the Data Processing Terms for Personal Data (which are incorporated by reference);
- (b) the security measures described in Cisco's Information Security Exhibit;
- (c) the Privacy Data Sheets applicable to the relevant Cisco Offer; and
- (d) privacy and data protection laws applicable to Cisco Offers.

7.3 You will ensure Your use of Cisco Offers (including collection, processing and use of Customer Content with Cisco Offers) complies with privacy and data protection laws applicable to Your Cisco Offers, including industry-specific requirements. You are also responsible for providing notice to, and getting consents from individuals whose data may be collected, processed, transferred and stored through Your use of Cisco Offers.

## 8. Ownership of intellectual property

8.1 Unless agreed in writing, nothing in these terms transfers ownership in any intellectual property rights. You keep ownership of Customer Content and Cisco keeps ownership of Cisco Offers and Cisco Content.

8.2 Cisco may use any feedback You provide in connection with Your use of Cisco Offers.

## 9. Intellectual property indemnity

9.1 Claims. Cisco will defend any third-party claim against You asserting that Your valid use of a Cisco Offer infringes a third party's patent, copyright or registered trademark (the "IP Claim"). Cisco will indemnify You against the final judgment entered by a court of competent jurisdiction or any settlements arising out of an IP Claim, if You:

- (a) promptly notify Cisco in writing of the IP Claim (but failure to promptly notify Cisco only limits Cisco's obligations to the extent it is prejudiced by the delay);
- (b) fully cooperate with Cisco in the defense of the IP Claim; and
- (c) grant Cisco the right to exclusively control the defense and settlement of the IP Claim, and any appeal.

Cisco does not have to reimburse You for attorney fees and costs incurred before Cisco receives notification of the IP Claim. You may retain Your own legal representation at Your own expense.

9.2 Additional remedies. If an IP Claim prevents or is likely to prevent You from accessing or using the applicable Cisco Offer, Cisco will either get the right for You to continue using the Cisco Offer or replace or modify the applicable Cisco Offer with non-infringing functionality that is at least equivalent. If Cisco determines those options are not reasonably available, then Cisco will provide a prorated refund for the impacted Cisco Offer.

9.3 Exclusions. Cisco has no duty regarding any IP Claim to the extent based on:

- (a) any designs, specifications or requirements provided by You, or on Your behalf;
- (b) modification of a Cisco Offer by You, or on Your behalf;
- (c) the amount or duration of use made of a Cisco Offer, revenue You earned, or services You offered;
- (d) combination, operation, or use of the Cisco Offer with non-Cisco products, software, content or business processes; or
- (e) Your failure to change or replace the Cisco Offer as required by Cisco.

9.4 To the extent allowed by law, this section 9 states Your only remedy regarding an IP Claim against You.

9.1 Claims. Cisco will defend any third-party claim against You asserting that Your valid use of a Cisco Offer infringes a third party's patent, copyright or registered trademark (the "IP Claim"). Cisco will indemnify You against the final judgment entered by a court of competent jurisdiction or any settlements arising out of an IP Claim, if You:

- (a) promptly notify Cisco in writing of the IP Claim (but failure to promptly notify Cisco only limits Cisco's obligations to the extent it is prejudiced by the delay);
- (b) fully cooperate with Cisco in the defense of the IP Claim; and
- (c) grant Cisco the right to exclusively control the defense and settlement of the IP Claim, and any appeal.

Cisco does not have to reimburse You for attorney fees and costs incurred before Cisco receives notification of the IP Claim. You may retain Your own legal representation at Your own expense.

9.2 Additional remedies. If an IP Claim prevents or is likely to prevent You from accessing or using the applicable Cisco Offer, Cisco will either get the right for You to continue using the Cisco Offer or replace or modify the applicable Cisco Offer with non-infringing functionality that is at least equivalent. If Cisco determines those options are not reasonably available, then Cisco will provide a prorated refund for the impacted Cisco Offer.

9.3 Exclusions. Cisco has no duty regarding any IP Claim to the extent based on:

- (a) any designs, specifications or requirements provided by You, or on Your behalf;
- (b) modification of a Cisco Offer by You, or on Your behalf;
- (c) the amount or duration of use made of a Cisco Offer, revenue You earned, or services You offered;
- (d) combination, operation, or use of the Cisco Offer with non-Cisco products, software, content or business processes; or
- (e) Your failure to change or replace the Cisco Offer as required by Cisco.

9.4 To the extent allowed by law, this section 9 states Your only remedy regarding an IP Claim against You.

## 10. Performance standards

10.1 Service Level Agreement. Cisco Offers will comply with applicable Service Level Agreements, as set out in the corresponding Offer Description.

10.2 Warranties. Cisco provides these warranties for Cisco Offers:

**Table 20. Cisco provides these warranties for Cisco Offers**

Warranty	Hardware	Software	Subscription Offers
<ul style="list-style-type: none"><li>• Cisco warrants that the Cisco Offer substantially complies with the Documentation as follows:</li><li>• (a) if the Cisco Offer is a Subscription Offer, starting from commencement of the service, for the duration of the services; and</li><li>• (b) if the Cisco Offer is Hardware or Software, for 90 days from shipment or longer as stated in Documentation, or as set out in <a href="#">Product Warranties</a> webpage.</li></ul>	YES	YES	YES
Cisco warrants it will use commercially reasonable efforts and methods to deliver the Cisco Offer free from Malicious Code.	N/A	YES	YES
Cisco warrants that the Cisco Offer is free from defects in material and workmanship for 90 days from shipment or longer as stated in Documentation or as set out in <a href="#">Product Warranties</a> webpage.	YES	N/A	N/A

To make a claim for breach of these warranties, promptly notify both Cisco and Cisco Partner (if they are Your Approved Source) within any specified warranty period.

10.3 Qualifications

- (a) You may have legal rights in Your country that prohibit or restrict the limitations set out in this section 10. This section 10 applies only to the extent permitted under applicable law.
- (b) Section 10.2 does not apply if Your breach of the General Terms contributes to the breach of warranty, or if the Cisco Offer:
  - (1) has not been used according to its Documentation;
  - (2) has been altered, except by Cisco or its authorized representative;
  - (3) has been subjected to abnormal or improper environmental conditions, accident or negligence, or installation or use inconsistent with Cisco's instructions or the terms on which it is supplied by Cisco;
  - (4) is provided under a Free Trial; or
  - (5) has not been provided by an Approved Source.

- (c) Your sole remedy for breach of a warranty under section 10.2 is, at Cisco's option, either:
- (1) repair or replacement of the applicable Cisco Offer; or
  - (2) a refund of either:
    - (A) the fees paid for Use Rights in the non-conforming Software;
    - (B) the fees paid for the period in which the Subscription Offer did not conform less any amounts paid or owed under a Service Level Agreement; or
    - (C) the fees paid for the non-conforming Hardware.
  - (d) Except as provided in Section 10.2 above, and to the extent allowed by law, Cisco makes no express or implied warranties of any kind regarding the Cisco Offers. This disclaimer includes any warranty, condition or other term as to merchantability, merchantable quality, fitness for purpose or use, course of dealing, usage of trade, or non-infringement. Cisco does not warrant that Cisco Offers will be secure, uninterrupted or error-free.

## 11. Liability

11.1 Excluded liability. Neither party is liable for:

- (a) indirect, incidental, reliance, consequential, special or exemplary damages; or
- (b) loss of actual or anticipated revenue, profit, business, savings, data, goodwill or use, business interruption, damaged data, wasted expenditure or delay in delivery (in all cases, whether direct or indirect).

11.2 Liability cap. Each party's entire liability for all claims relating to these terms will not exceed the greater of: (a) the fees paid to Cisco for the specific Cisco Offer that is the subject of the claim in the 12 months before the first incident giving rise to such liability; or (b) \$100,000 USD. This cap is cumulative for all claims (not per incident) and applies collectively to each party and its Affiliates (not per Affiliate).

11.3 Unlimited liability. Nothing in this section 11 limits or excludes liabilities that cannot be excluded or limited under applicable law, or for:

- (a) bodily injury or death resulting directly from the other party's negligence;
- (b) fraudulent misrepresentation or wilful misconduct;
- (c) breach of confidentiality obligations, unless the breach relates to section 7 (Privacy and security);
- (d) failure to pay for Cisco Offers;
- (e) misuse or misappropriation by a party of the other party's intellectual property rights; or
- (f) failure to comply with export control obligations.

## 12. Termination

12.1 Material breach. Either party may provide written notice to the other party if the other party materially breaches these terms or any written terms otherwise agreed under an affected Order. If the breach remains uncured after 30 days of the date of that notice, the non-breaching party may immediately terminate the affected Orders, in whole or in part.

12.2 Termination for Compliance with Laws. Cisco may terminate these terms and affected Orders immediately upon written notice if continued provision of the Cisco Offers will result in a violation of section 13.7 (Compliance with Laws).

12.3 Effect of termination or expiration. You will Return applicable Cisco Offers (except any Cisco Offer in which title has transferred to You) at the end of Your Use Term or upon termination of an Order.

## 13. General provisions

13.1 Survival. Sections 5 (Paying Your Approved Source), 6 (Confidentiality), 7 (Privacy and security), 8 (Ownership of intellectual property), 9 (IP Indemnity), 10 (Performance standards), 11 (Liability), 12 (Termination) and 13 (General provisions) survive termination of these terms.

13.2 No agency. These terms do not create any agency, partnership, joint venture, or franchise relationship.

13.3 Assignment and subcontracting.



(a) Except as set out below, neither party may assign or novate these terms in whole or in part without the other party's written consent which will not be unreasonably withheld. Cisco may assign these terms in connection with the sale of a part of its business, or to its Affiliates if it provides prior written notice to You.

(b) Cisco may subcontract any performance associated with any Cisco Offer to third parties if such subcontract is consistent with these terms and does not relieve Cisco of any of its obligations under these terms.

13.4 Third party beneficiaries. These terms do not grant any right or cause of action to any third party.

13.5 Use records. You will keep reasonable records of your use of the Cisco Offers. You will let Cisco and its auditors who are under a written obligation of confidentiality access records of Your use of the Cisco Offers (including books, systems, and accounts) within 30 days' notice from Cisco. Cisco may not give this notice more than once in any 12-month period and will conduct any audit during Your normal business hours. If the verification process reveals underpayment of fees, You will pay these fees within 30 days.

13.6 Changes to these terms. The version of the General Terms applicable to Your Order is the version published at the [Cisco General Terms](#) webpage when the Order is placed. If Cisco changes these terms or any of its parts, these changes will be published at the [Cisco General Terms](#) webpage. These changes will only apply to Cisco Offers Ordered or renewed after the date of the change.

13.7 Compliance with laws

(a) General. Cisco will comply with all applicable laws relating to providing Cisco Offers under these terms. You will comply with all applicable laws relating to Your receipt and use of Cisco Offers, including sector-specific requirements and obtaining required licenses or permits (if any).

(b) Trade Compliance. Cisco Offers are subject to US and other export control and sanctions laws around the world. These laws govern the use, transfer, export and re-export of Cisco Offers. Each party will comply with such laws and obtain all licenses or authorizations it is required to maintain. Please refer to Cisco's trade compliance policies at the [General Export Compliance](#) webpage.

13.8 Governing law and venue. These terms, and any disputes arising from them, are subject to the governing law and exclusive jurisdiction and venue listed below, based on Your primary place of business. Each party consents and submits to the exclusive jurisdiction of the courts in the listed venue. These laws apply despite conflicts of laws rules or the United Nations Convention on Contracts for the International Sale of Goods. Despite the below, either party may seek interim injunctive relief in any court of appropriate jurisdiction regarding any alleged breach of confidentiality obligations or intellectual property or proprietary rights.

**Table 21. Jurisdiction and Venue**

<b>Your Primary Place of Business</b>	<b>Governing Law</b>	<b>Jurisdiction and Venue</b>
United States, Latin America or the Caribbean, or a location not specified below	State of California, United States	Superior Court of California, County of Santa Clara and Federal Courts of the Northern District of California
Africa, Asia*, Europe*, Middle East, Oceania*	England	English Courts
Australia	State of New South Wales, Australia	State and Federal Courts in New South Wales
Canada	Province of Ontario, Canada	Courts of the Province of Ontario
Mainland China	People's Republic of China	Hong Kong International Arbitration Center
Italy	Italy	Court of Milan
Japan	Japan	Tokyo District Court of Japan

\* Excluding locations listed separately in this table.

If You are a US State, Local and Education ("SLED") Government end user, these terms, and any disputes arising from them, are subject to the laws of the primary jurisdiction in which You are located.

If You are a US Federal Government end user, these terms, and any disputes arising from them, are subject to the laws of the United States.

13.9 US Government end users

(a) US SLED Government. These terms govern all access to Software, Subscription Offers and Documentation by US SLED Government end users. No other rights are granted by Cisco.

(b) US Federal Government. The Software, Subscription Offers and Documentation are considered “commercial computer software” and “commercial computer software documentation” under FAR 12.212 and DFARS 227.7202. These terms govern all access to Software, Subscription Offers and Documentation by US Federal Government end users. No other rights are granted by Cisco, but any inconsistency in these terms with federal procurement regulations is not enforceable against the US Federal Government.

13.10 Notice. Unless provided in these terms, applicable Offer Description, or an Order, notices to Cisco (a) should be sent to Cisco Systems, Legal Department, 170 West Tasman Drive, San Jose, CA 95134 or by email to [contract-notice@cisco.com](mailto:contract-notice@cisco.com), and (b) are considered effective (i) upon delivery, if personally delivered, (ii) the next day, if sent by overnight mail, (iii) 3 business days after deposit, postage prepaid, if mailed, or (iv) the same day receipt is acknowledged, if sent by e-mail. Cisco may deliver notice to You under these terms via email or regular mail, but it may provide notices of a general nature applicable to multiple customers on [cisco.com](http://cisco.com).

13.11 Force majeure. Neither party is responsible for delay or failure to perform its obligations to the extent caused by events beyond a party’s reasonable control including severe weather events, acts of God, supply shortages, labor strikes, epidemic, pandemic, acts of government, war, acts of terrorism or the stability or availability of utilities (including electricity and telecommunications). The affected party must make commercially reasonable efforts to mitigate the impact of the force majeure event.

13.12 No waiver. Failure by either party to enforce any right under these terms will not waive that right.

13.13 Severability. If any term in these terms is invalid or unenforceable, then the rest of these terms will continue with full force and effect to the extent possible.

13.14 Entire agreement. These terms are the complete agreement between the parties regarding the subject of these terms and replace all previous communications, understandings or agreements (whether written or oral).

13.15 Translations. Cisco may provide local language translations of these terms in some locations. Those translations are provided for informational purposes only. If there is any inconsistency in those translations, the English version of these terms will prevail.

13.16 No publicity. Neither party will issue any press release or other publications regarding Your use of Cisco Offers without the other party’s advance written permission.

13.17 Order of precedence.

(a) If there is any conflict between these General Terms, Supplemental Terms or any Offer Descriptions, the order of precedence (from highest to lowest) is:

- (1) Regional terms;
- (2) Data Processing Terms;
- (3) Offer Descriptions;
- (4) Supplemental Terms (other than Regional Terms);
- (5) these General Terms; then
- (6) any applicable Cisco policy referenced in these General Terms.

(b) As between You and Cisco, these terms prevail over any inconsistencies with Your contract with any Cisco Partner.

## 14. Definitions

**Table 22. Definitions**

Term	Meaning
Affiliate	Any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where “control” means to: (a) own over 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through voting rights or other lawful means (e.g., a contract that allows control).
Approved Source	Cisco, a Cisco Partner, or a fulfillment agent (e.g., public cloud marketplaces) as may be appointed by Cisco from time to time.
Authorized Users	Your users including Affiliates, Your third-party service providers, and each of their respective Users.

**Table 22. Definitions (continued)**

<b>Term</b>	<b>Meaning</b>
Buying Program	Cisco's consumption-based programs for buying Cisco Offers such as the Cisco Enterprise Agreement.
Cisco, we, our or us	Cisco Systems, Inc. or its applicable Affiliates.
Cisco Content	Systems Information and data, materials or other content provided by Cisco directly or through Your Approved Source to You as part of Your access to Cisco Offers.
Cisco Offer	Cisco-branded (a) Hardware, (b) Use Rights in Software or Cloud Services, (c) technical support included in a Subscription Offer and (d) incidental technology and resources.
Cisco Partner	A Cisco authorized reseller, distributor, systems integrator or other third party authorized by Cisco to sell Cisco Offers.
Cloud Service	An on-demand service provided by Cisco accessible via the internet and provides software, platform, infrastructure and network products and services on an 'as-a-service' basis as described in the applicable Offer Description.
Confidential Information	Non-public proprietary information of the discloser obtained by the recipient in connection with these terms, which: (a) is conspicuously marked as confidential if written or clearly stating the information is confidential when (or promptly after) it is verbally disclosed; or (b) is information which by its nature should reasonably be considered confidential whether disclosed in writing or orally.
Customer Content	As defined in the Data Brief at the <a href="#">Customer Content - Data Brief</a> webpage.
Data	Personal Data, Customer Content and Systems Information.
Data Briefs	Documents describing each type of Data (e.g., Personal Data, Customer Content and Systems Information) that Cisco Offers collect, how it is collected, and when it is used, available at the <a href="#">Trust Portal</a> webpage.
Data Processing Terms	Cisco's data processing terms in the <a href="#">Data Protection Agreement</a> , or terms agreed between You and Cisco covering the same scope.
Documentation	The technical specifications and use materials officially published by Cisco specifying the functionalities and capabilities of the applicable Cisco Offer as updated from time to time.
Free Trial	As defined in section 3.1 (Accessing free trials).
Free Trial Period	As defined in Section 3.1 (Accessing free trials).
Hardware	Tangible Cisco-branded hardware products as generally available on the Price List. Hardware does not include any tangible product listed on the Price List in the name of a third party.
Information Security Exhibit	A document describing the security measures that Cisco implements to secure Personal Data and Customer Content, available at the <a href="#">Information Security Exhibit</a> webpage.
Malicious Code	Code designed or intended to disable or impede the normal operation of, or provide unauthorized access to, networks, systems, Software or Cloud Services other than as intended by the Cisco Offer (e.g., as part of Cisco's security products).

**Table 22. Definitions (continued)**

<b>Term</b>	<b>Meaning</b>
Offer Description	A document published by Cisco as an 'Offer Description' that has more information or related terms specific to a Cisco Offer or Buying Program, available at the <a href="#">Product Specific Terms</a> webpage.
Order	The transaction through which You acquire a Cisco Offer from an Approved Source, including through buying and ordering documents, signing an agreement or statement of work, or transacting through an online ordering tool or marketplace.
Personal Data	Any information about, or relating to, an identifiable individual. It includes any information that can be linked to an individual or used to, directly or indirectly, identify an individual, natural person. Further information regarding Personal Data is on the <a href="#">Personal Data - Data Brief</a> webpage.
Price List	The price lists published at Cisco.com corresponding to the Cisco entity that sells the applicable Cisco Offer.
Privacy Data Sheet	The privacy data sheet applicable to a Cisco Offer available on the <a href="#">Trust Portal - Privacy Data Sheet</a> webpage.
Return	Stopping all use of, destroying or returning applicable Cisco Offers to Your Approved Source, as directed by Cisco or Your Approved Source.
Service Level Agreement	The service level agreement applicable to a Subscription Offer (if applicable) as set out in the applicable Offer Description.
Software	Cisco-branded computer programs, including Upgrades and firmware.
Subscription Offer	Cisco Offers provided on a term, or subscription, basis under Your Order.
Supplemental Terms	Any additional terms applicable to Your Order (including those applying to a specific region or Buying Program).
Systems Information	As defined in the <a href="#">Systems Information – Data Brief</a> webpage.
Transfer Policies	Cisco policies for movement of Use Rights as set out in the <a href="#">Cisco Software Transfer and Re-licensing Policy</a> and the <a href="#">Software License Portability Policy</a> .
Upgrades	All updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software.
Use Term	The period You may exercise Use Rights in the Cisco Offer under Your Order.
Use Rights	As set out in section 2.1.
You, Your	The individual or legal entity acquiring access to Cisco Offers.

## Important Links

Links to various Cisco data briefs, agreements, and policies.

Here are some important links related to Cisco data briefs, agreements, and policies:

- [Customer Content - Data Brief](#)
- [Trust Portal](#)
- [Data Protection Agreement](#)
- [Information Security Exhibit](#)
- [Product Specific Terms](#)

- [Personal Data - Data Brief](#)
- [Trust Portal - Privacy Data Sheet](#)
- [Systems Information – Data Brief](#)
- [Cisco Software Transfer and Re-licensing Policy](#)
- [Software License Portability Policy](#)

## Citrix Workspace End User License Agreement

1. Use of this component is subject to the Citrix license or terms of service covering the Citrix product(s) and/or service(s) with which you will be using this component. This component is licensed for use only with such Citrix product(s) and/or service(s);

- 1. (General License Grant) above, You may permit Your Third Party Agents to access, use and/or operate the Software on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this EULA and any breach of this EULA by a Third Party Agent shall be deemed to be a breach by You
- 2. Third Party Agents. Under the License granted to You in Section;
- 3. Copying Permitted. You may copy the Software and Documentation as necessary to install and run the quantity of copies licensed, but otherwise for archival purposes only
- 4. Benchmarking. You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or otherwise distribute the results of such studies to third parties as follows: (a) if with respect to VMware's Workstation or Fusion products, only if You provide a copy of Your study to [benchmark@vmware.com](mailto:benchmark@vmware.com) prior to distribution; (b) if with respect to any other Software, only if VMware has reviewed and approved of the methodology, assumptions and other parameters of the study (please contact VMware at [benchmark@vmware.com](mailto:benchmark@vmware.com) to request such review and approval) prior to such publication and distribution
- 5. VMware Tools. You may distribute the VMware Tools to third parties solely when installed in a Guest Operating System within a Virtual Machine. You are liable for compliance by those third parties with the terms and conditions of this EULA
- 6. Open Source Software. Notwithstanding anything herein to the contrary, Open Source Software is licensed to You under such OSSs own applicable license terms, which can be found in the `open_source_licenses.txt` file, the Documentation or as applicable, the corresponding source files for the Software available at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html). These OSS license terms are consistent with the license granted in Section 2 (License Grant), and may contain additional rights benefiting You. The OSS license terms shall take precedence over this EULA to the extent that this EULA imposes greater restrictions on You than the applicable OSS license terms. To the extent the license for any Open Source Software requires VMware to make available to You the corresponding source code and/or modifications (the;Source Files;), You may obtain a copy of the applicable Source Files from VMware's website at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html) or by sending a written request, with Your name and address to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date You acquired this Software.

### RESTRICTIONS; OWNERSHIP

- 1. License Restrictions. Without VMware's prior written consent, You must not, and must not allow any third party to: (a) use Software in an application services provider, service bureau, or similar capacity for third parties, except that You may use the Software to deliver hosted services to Your Affiliates; (b) disclose to any third party the results of any benchmarking testing or comparative or competitive analyses of VMware's Software done by or on behalf of You, except as specified in Section 2.4 (Benchmarking); (c) make available Software in any form to anyone other than Your employees or contractors reasonably acceptable to VMware and require access to use Software on behalf of You in a matter permitted by this EULA, except as specified in Section 2.2 (Third Party Agents); (d) transfer or sublicense Software or Documentation to an Affiliate or any third party, except as expressly permitted in Section 12.1 (Transfers; Assignment); (e) use Software in conflict with the terms and restrictions of the Software's licensing model and other requirements specified in Product Guide and/or VMware quote; (f) except to the extent permitted by applicable mandatory law, modify, translate, enhance, or create derivative works from the Software, or reverse engineer, decompile, or otherwise attempt to derive source code from the Software, except as specified in Section 3.2 (Decompilation); (g) remove any copyright or other proprietary notices on or in any copies of Software; or (h) violate or circumvent any technological restrictions within the Software or specified in this EULA, such as via software or services

;3.2. Decompilation. Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the Territory give You the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, You must first request such information from VMware, provide all reasonably requested information to allow VMware to assess Your claim, and VMware may, in its discretion, either provide such interoperability information to You, impose reasonable conditions, including a reasonable fee, on such use of the Software, or offer to provide alternatives to ensure that VMware's proprietary rights in the Software are protected and to reduce any adverse impact on VMware's proprietary rights

;3.3. Ownership. The Software and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Software and Documentation shall be limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Software or any related Intellectual Property Rights are implied.

You are not authorized to use (and shall not permit any third party to use) the Software, Documentation or any portion thereof except as expressly authorized by this EULA or the applicable Order.

VMware reserves all rights not expressly granted to You. VMware does not transfer any ownership rights in any Software

;3.4. Guest Operating Systems. Certain Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that You are responsible for obtaining and complying with any licenses necessary to operate any such third- party software

;4. ORDER. Your Order is subject to this EULA. No Orders are binding on VMware until accepted by VMware. Orders for Software are deemed to be accepted upon VMware's delivery of the Software included in such Order. Orders issued to VMware do not have to be signed to be valid and enforceable

;5. RECORDS AND AUDIT. During the License Term for Software and for two (2) years after its expiration or termination, You will maintain accurate records of Your use of the Software sufficient to show compliance with the terms of this EULA. During this period, VMware will have the right to audit Your use of the Software to confirm compliance with the terms of this EULA. That audit is subject to reasonable notice by VMware and will not unreasonably interfere with Your business activities. VMware may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. You will reasonably cooperate with VMware and any third party auditor and will, without prejudice to other rights of VMware, address any non-compliance identified by the audit by promptly paying additional fees. You will promptly reimburse VMware for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the Software fees payable by You for the period audited, or that You have materially failed to maintain accurate records of Software use

;6. SUPPORT AND SUBSCRIPTION SERVICES. Except as expressly specified in the Product Guide, VMware does not provide any support or subscription services for the Software under this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software developed by VMware unless you separately purchase VMware support or subscription services. These support or subscription services are subject to the Support Services Terms

## 7. WARRANTIES

;7.1. Software Warranty, Duration and Remedy. VMware warrants to You that the Software will, for a period of ninety (90) days following notice of availability for electronic download or delivery (;Warranty Period;), substantially conform to the applicable Documentation, provided that the Software: (a) has been properly installed and used at all times in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than VMware or its authorized representative.

VMware will, at its own expense and as its sole obligation and Your exclusive remedy for any breach of this warranty, either replace that Software or correct any reproducible error in that Software reported to VMware by You in writing during the Warranty Period. If VMware determines that it is unable to correct the error or replace the Software, VMware will refund to You the amount paid by You for that Software, in which case the License for that Software will terminate

;7.2. Software Disclaimer of Warranty. OTHER THAN THE WARRANTY ABOVE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES UNDER THIS EULA, AND DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING OR PERFORMANCE, OR USAGE OF TRADE. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT IT WILL MEET YOUR REQUIREMENTS

## 8. INTELLECTUAL PROPERTY INDEMNIFICATION

;8.1. Defense and Indemnification. Subject to the remainder of this Section 8 (Intellectual Property Indemnification), VMware shall defend You against any third party claim that the Software infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to the extent that such countries are part of the Territory for the License ('Infringement Claim') and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement. The foregoing obligations are applicable only if You: (i) promptly notify VMware in writing of the Infringement Claim; (ii) allow VMware sole control over the defense for the claim, any settlement negotiations and any related action challenging the validity of the allegedly infringed patent, trademark, or copyright; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware

8.2 Remedies. If the alleged infringing Software become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense, do one of the following: (a) procure the rights necessary for You to make continued use of the affected Software; (b) replace or modify the affected Software to make it non-infringing;

or (c) terminate the License to the affected Software and discontinue the related support services, and, upon Your certified deletion of the affected Software, refund: (i) the fees paid by You for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date such Software was delivered; and (ii) any pre-paid service fee attributable to related support services to be delivered after the date such service is stopped. Nothing in this Section 8.2 (Remedies) shall limit VMware's obligation under Section 8.1 (Defense and Indemnification) to defend and indemnify You, provided that You replace the allegedly infringing Software upon VMware's making alternate Software available to You and/or You discontinue using the allegedly infringing Software upon receiving VMware's notice terminating the affected License

;8.3. Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 8 (Intellectual Property Indemnification) or otherwise with respect to any claim based on: (a) a combination of Software with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer VMware version would have avoided the infringement; (d) any modification to the Software made without VMware's express written approval; (e) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into Software listed on VMware's commercial price list; or (f) any Software provided on a no charge, beta or evaluation basis. THIS SECTION 8 (INTELLECTUAL PROPERTY INDEMNIFICATION) STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS

## 9. LIMITATION OF LIABILITY

9.1. Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS EULA WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE GREATER OF THE LICENSE FEES YOU PAID FOR THE SOFTWARE GIVING RISE TO THE CLAIM OR \$5000. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE

9.2. Further Limitations. VMware's licensors shall have no liability of any kind under this EULA and VMware's liability with respect to any third party software embedded in the Software shall be subject to Section 9.1 (Limitation of Liability). You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises

## 10. TERMINATION

10.1. EULA Term. The term of this EULA begins on the notice of availability for electronic download or delivery of the Software and continues until this EULA is terminated in accordance with this Section 10

10.2. Termination for Breach. VMware may terminate this EULA effective immediately upon written notice to You if: (a) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; or (b) You breach any other provision of this EULA and fail to cure within thirty (30) days after receipt of VMware's written notice thereof

10.3. Termination for Insolvency. VMware may terminate this EULA effective immediately upon written notice to You if You: (a) terminate or suspend your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding

10.4. Effect of Termination. Upon VMware's termination of this EULA: (a) all Licensed rights to all Software granted to You under this EULA will immediately cease; and (b) You must cease all use of all Software, and return or certify destruction of all Software and License Keys (including copies) to VMware, and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Any provision will survive any termination or expiration if by its nature and context it is intended to survive, including Sections 1 (Definitions), 2.6 (Open Source Software), 3 (Restrictions; Ownership), 5 (Records and Audit), 7.2 (Software Disclaimer of Warranty), 9 (Limitation of Liability), 10 (Termination), 11 (Confidential Information) and 12 (General)

## 11. CONFIDENTIAL INFORMATION

11.1. Definition. 'Confidential Information' means information or materials provided by one party ('Discloser') to the other party ('Recipient') which are in tangible form and labelled 'confidential' or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding VMware's pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software

11.2. Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this EULA; or (b) in connection with the parties' ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by this EULA, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for

purposes of this EULA and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care

11.3.Exceptions. Recipient's obligations under Section 11.2 (Protection) with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser's Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest or limit the scope of such required disclosure

11.4.Data Privacy. You agree that VMware may process technical and related information about Your use of the Software which may include internet protocol address, hardware identification, operating system, application software, peripheral hardware, and non-personally identifiable Software usage statistics to facilitate the provisioning of updates, support, invoicing or online services and may transfer such information to other companies in the VMware worldwide group of companies from time to time. To the extent that this information constitutes personal data, VMware shall be the controller of such personal data. To the extent that it acts as a controller, each party shall comply at all times with its obligations under applicable data protection legislation

## 12.GENERAL

12.1.Transfers; Assignment. Except to the extent transfer may not legally be restricted or as permitted by VMware's transfer and assignment policies, in all cases following the process set forth at [www.vmware.com/support/policies/licensingpolicies.html](http://www.vmware.com/support/policies/licensingpolicies.html), You will not assign this EULA, any Order, or any right or obligation herein or delegate any performance without VMware's prior written consent, which consent will not be unreasonably withheld. Any other attempted assignment or transfer by You will be void. VMware may use its Affiliates or other sufficiently qualified subcontractors to provide services to You, provided that VMware remains responsible to You for the performance of the services

12.2. Notices. Any notice delivered by VMware to You under this EULA will be delivered via mail, email or fax

12.3. Waiver. Failure to enforce a provision of this EULA will not constitute a waiver

12.4. Severability. If any part of this EULA is held unenforceable, the validity of all remaining parts will not be affected

12.5. Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this EULA. You acknowledge that the Software is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and accompanying documentation are deemed to be 'commercial computer software' and 'commercial computer software documentation', respectively, pursuant to DFARS Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and documentation by or for the U.S. Government shall be governed solely by the terms and conditions of this EULA ;

12.6. Construction. The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word 'including' means 'including but not limited to' ;

12.7. Governing Law. This EULA is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), and the federal laws of the United States. To the extent permitted by law, the state and federal courts located in Santa Clara County, California will be the exclusive jurisdiction for disputes arising out of or in connection with this EULA. The U.N. Convention on Contracts for the International Sale of Goods does not apply ;

12.8. Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it ;

12.9. Order of Precedence. In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following order of precedence shall apply unless otherwise set forth in an enterprise license agreement: (a) the Product Guide, (b) this EULA and (c) the Order. With respect to any inconsistency between this EULA and an Order, the terms of this EULA shall supersede and control over any conflicting or additional terms and conditions of any purchase order, acknowledgement or confirmation or other document issued by You ;

12.10. Entire Agreement. This EULA, including accepted Orders and any amendments hereto, and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous



communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This EULA may be amended only in writing signed by authorized representatives of both parties

12.11. Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department 'This is a legal agreement (;AGREEMENT;) between the end-user customer (;you;), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as;CITRIX;). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter;PRODUCT;) and maintenance (hereinafter;MAINTENANCE;) determines the providing entity as identified at <https://www.citrix.com/buy/licensing/citrix-providing-entities.html>. BY INSTALLING AND/OR USING THE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT.'

## 1. PRODUCT LICENSES

a. End User Licenses. Citrix hereby grants Customer a non- exclusive worldwide license to use the software in a software PRODUCT and the software installed in an appliance PRODUCT under the license models identified at <https://www.citrix.com/buy/licensing/product.html>. Unless otherwise noted, each product license may be loaded on only a single license server, appliance or appliance instance, as applicable. Any experimental features delivered with such software will be identified and are licensed only for internal testing purposes. Notwithstanding anything set forth in this AGREEMENT or at the referenced website, your use of open source software shall in all ways be exclusively governed by the open source license indicated as applicable to the code at <https://www.citrix.com/buy/licensing/open-source.html>. ' Your license to software in a Software or Appliance PRODUCT will be activated by license keys that allow use of the PRODUCT in increments defined by the license model purchased (;License Keys;). ;Software means a Citrix proprietary and/or open source software program in object code form licensed hereunder. ;Appliance; means a hardware appliance with installed Software. License Keys for other CITRIX products or other editions of the same PRODUCT may not be used to increase the allowable use for your edition of the PRODUCT.

b. Partner Demo. If a Software PRODUCT is labeled ;Partner Demo,; notwithstanding any term to the contrary in this AGREEMENT, your license permits use only if you are a current CITRIX authorized distributor or reseller, and then only for demonstration, test, or evaluation purposes in support of your end-user customers, and not for any other purpose, including without limitation customer training or production purposes. Note that a Partner Demo PRODUCT may disable itself upon the expiration of the License Key. In no event may a Partner Demo PRODUCT be used beyond expiration.

c. Evaluation. If a PRODUCT is labeled ;Evaluation,; notwithstanding any term to the contrary in this AGREEMENT, your license permits use only if you are an end-user customer and then only for your internal demonstration, test, or evaluation purposes, and not for any other purpose, including without limitation production purposes. Your license is for ninety (90) days with no right to MAINTENANCE, the Limited Warranty, or Infringement Indemnification. Note that an Evaluation PRODUCT may disable itself upon the expiration of the License Key. In no event may an Evaluation PRODUCT be used beyond expiration. If the Evaluation PRODUCT is an appliance, it must be returned upon such expiration.

d. Archive Copy. You may make one (1) copy of the software in a Software or Appliance PRODUCT in machine-readable form solely for backup, provided that you reproduce all proprietary notices on the copy.'

## 2. MAINTENANCE.

The MAINTENANCE plan applicable to this PRODUCT is identified at <https://www.citrix.com/buy/licensing/product.html> and plan entitlements and requirements are explained at <https://www.citrix.com/support/programs.html>. Entitlements may include cloud services that shall be delivered under the terms of the End User Services Agreement at <https://www.citrix.com/buy/licensing/agreements.html>. MAINTENANCE is required at the time of PRODUCT purchase and must be purchased separately. MAINTENANCE is available for an initial one (1) year term and may automatically renew or be extended by your purchase of available annual renewals (the;MAINTENANCE Term;).' 'The MAINTENANCE offering you purchase determines how renewals work. In the event your offering includes automatic renewals, should you wish to allow MAINTENANCE to expire at the end of your then current term, you must provide Citrix thirty (30) days advance written notice. MAINTENANCE for a Software or Appliance PRODUCT begins upon delivery of the License Keys. During the initial or a renewal MAINTENANCE Term, CITRIX will make any Updates for the PRODUCT covered by the plan available to you. An ;Update; shall mean a generally available release of the same edition of the Software for the same PRODUCT that Citrix may make available from time to time. CITRIX is not obligated to make any Updates available. Updates shall be subject to the terms of this AGREEMENT, except that Updates are not covered by the Limited Warranty applicable to the PRODUCT, to the extent permitted by applicable law.' 'You acknowledge that CITRIX may develop and market new or different software or appliance offerings or editions of the PRODUCT that use portions of the PRODUCT and that perform all or part of the functions performed by the PRODUCT. Nothing contained in this AGREEMENT shall give you any rights with respect to such new or different offerings or editions. The MAINTENANCE plan may be purchased for the PRODUCT until it is no longer offered in accordance with the applicable CITRIX PRODUCT Lifecycle Support Policy posted at <https://www.citrix.com/support/product-lifecycle.html>. Any deliveries of Updates shall be electronic. The MAINTENANCE plan includes technical support, and may include online services, and, for hardware only, an extended hardware warranty, as stated at <https://www.citrix.com/support/programs.html>. The offering you purchase determines your entitlement and usage rights.' 'In addition to your MAINTENANCE plan, you may also

purchase CITRIX consulting services as may be available (including installation services, remote monitoring services or technical consulting).';CITRIX' provision of technical support or consulting services is predicated upon the following responsibilities being fulfilled by you: (i) you will designate a primary administrative contact for technical support;(i) you will designate a primary administrative contact for technical support; (ii) you agree to perform reasonable problem determination activities and reasonable problem resolution activities as suggested by CITRIX; (iii) you are responsible for implementing procedures necessary to safeguard the integrity and security of software and data from unauthorized access and for reconstructing any lost or altered files resulting from catastrophic failures;;(iv) you are responsible for procuring, installing, and maintaining all equipment, telephone lines, communications interfaces, and other hardware at your site and providing CITRIX with access to your facilities as required to operate the PRODUCT and permitting CITRIX to perform the service; and (v) you are required to implement all currently available and applicable software hotfixes, hotfix rollup packs, and service packs or their equivalent for the PRODUCT in a timely manner. CITRIX is not required to provide any technical support for problems arising out of;;(i) your or any third party's alterations or additions to the PRODUCT, operating system or environment; (ii) CITRIX provided alterations or additions to the PRODUCT that do not address Errors or Defects; (iii) any functionality not defined in the user documentation published by CITRIX and included with the PRODUCT (hereinafter 'Documentation');; '(iv) use of a Software PRODUCT on a processor or peripherals other than the processor and peripherals defined in the Documentation; (v) any PRODUCT that has reached End-of-Life; and (vi) any consulting deliverables from CITRIX, you or any third party. An ;Error; is defined as a failure in the PRODUCT to materially conform to the functionality defined in the Documentation. A ;Defect; is defined as a failure in the PRODUCT to conform to the specifications in the Documentation. In situations where CITRIX cannot provide a satisfactory resolution to your critical problem through normal technical support methods, CITRIX may engage its product development team to create a private fix.';Private fixes are designed to address your specific situation and may not be further distributed by you. CITRIX retains all right, title, and interest in and to all fixes, packs and their equivalent. Any private fixes are not provided as part of the PRODUCT under the terms of this AGREEMENT and they are not covered by the Limited Warranty or Infringement Indemnification applicable to the PRODUCT, to the extent permitted by applicable law. With respect to CITRIX consulting services, all intellectual property rights in all deliverables, pre-existing works and derivative works of such pre-existing works, as well as developments made, conceived, created, discovered, invented, or reduced to practice in the performance of the consulting services are and shall remain the sole and absolute property of CITRIX, subject to a worldwide, non- exclusive license to you for internal use

3. DESCRIPTION OF OTHER RIGHTS, LIMITATIONS, AND OBLIGATIONS. Except as expressly set forth in Section 13, you may not transfer, rent, timeshare, grant rights in or lease the PRODUCT except to the extent such foregoing restriction is prohibited by applicable mandatory law. Any attempt to do so in violation of this prohibition shall be void. If you purchased or otherwise received replacement License Keys as part of a PRODUCT upgrade or trade-up, or a new product release with new product licenses under MAINTENANCE, you agree to destroy the original License Keys and retain no copies after installation of the new License Keys and PRODUCT. Solely for the purpose of migrating users, you are permitted a ninety (90) day grace period to run both your new and old License Keys in production. This period begins with your purchase of the upgrade or trade-up, or with your download of the new release under MAINTENANCE. You shall provide the serial numbers of the original License Keys and corresponding replacement License Keys to the reseller and, upon request, directly to CITRIX, for tracking purposes;In the event you make a transfer of the PRODUCT in the EU or EER, to the extent permitted by law and notwithstanding the terms of this AGREEMENT, you must uninstall the PRODUCT and License Keys, cease your use, transfer them to the transferee and retain no copies. You are responsible for ensuring that the transferee accepts the terms of this AGREEMENT. You must provide evidence that the conditions for a lawful transfer of the PRODUCT are met. All Limited Warranty, MAINTENANCE and Infringement Indemnification rights will terminate automatically upon such transfer and will not be available to the transferee, including the ability to purchase MAINTENANCE. You must comply with applicable export laws with respect to such a transfer. You may not modify, translate, reverse engineer, decompile, disassemble, create derivative works based on or copy the PRODUCT, except as expressly licensed in this AGREEMENT or to the extent such foregoing restriction is expressly prohibited by applicable mandatory law;You may not remove any proprietary notices, labels or marks on the PRODUCT. If you are a Citrix competitor for the relevant PRODUCT, you may not use the PRODUCT directly or indirectly for competitive benchmarking or other competitive analysis, unless permitted under applicable law. Notwithstanding the foregoing, this AGREEMENT shall not prevent or restrict you from exercising additional or different rights to any portions of the PRODUCT that are open source software. To the extent permitted by applicable law, you agree to allow CITRIX to audit your compliance pursuant to the terms explained at: <https://www.citrix.com/about/legal/product-license-compliance.html>. With respect to your purchase of a product trade-up or upgrade, or your implementation of a product release with new product licenses under MAINTENANCE, you are permitted a 90-day grace period to run both your new and the old PRODUCT licenses in production. This period runs from your purchase of the trade-up or upgrade, and from your download of the new release under your MAINTENANCE program 'You agree to destroy the old licenses and retain no copies after the grace period. Certain PRODUCTS include a license overdraft feature that enables you to use a limited number of additional licenses to prevent access denial. Any overdraft feature is offered as a convenience, not as a license entitlement. Any overdraft licenses used must be purchased within thirty (30) days of first use. Note that a PRODUCT may be provided with identified experimental features which are not part of the PRODUCT and which are not covered by MAINTENANCE and the Limited Warranty. Such features are offered ;AS IS; and may never become part of the PRODUCT or any CITRIX commercial product. Citrix makes no representations or certifications with respect to experimental features.ALL RIGHTS IN THE PRODUCT NOT EXPRESSLY GRANTED ARE RESERVED BY CITRIX OR ITS LICENSORS.CITRIX and/or its licensors own and retain all title and ownership of all intellectual property rights in and to the PRODUCT, including any adaptations, modifications, translations, derivative works or copies, and any relating to the design, manufacture, or operation of the same.' '

4. INFRINGEMENT INDEMNIFICATION. In the event of any claim, suit, or proceeding brought against you based on an allegation that a PRODUCT, experimental features or consulting deliverable hereunder (excluding open source software) infringes upon any patent, copyright or trade secret of any third party (Infringement Claim), CITRIX shall defend, or at its option, settle, such Infringement Claim, and shall pay all costs (including reasonable attorneys fees) associated with the defense of such Infringement Claim, and all damages finally awarded or settlements undertaken by CITRIX in resolution of such Infringement Claim, provided you: (i) promptly notify CITRIX in writing of your notification or discovery of an Infringement Claim such that CITRIX is not prejudiced by any delay in such notification; (ii) give CITRIX sole control over the defense or settlement of the Infringement Claim; and (iii) provide reasonable assistance in the defense of the same. Following notice of an Infringement Claim, or if CITRIX believes such a claim is likely, CITRIX may at its sole expense and option: (i) procure for you the right to continue to use the alleged infringing PRODUCT, experimental feature or consulting deliverable; (ii) replace or modify the PRODUCT, experimental feature or consulting deliverable to make it non-infringing; or (iii) accept return of the PRODUCT, experimental feature or consulting deliverable and, for the PRODUCT, provide you with a prorated refund for the PRODUCT, using a three (3) year straight line depreciation basis for the PRODUCT, or, for the consulting deliverable, refund payments made for the deliverable; (ii) any modification of the PRODUCT, experimental feature or consulting deliverable by you or at your direction; (iii) your combination of the PRODUCT, experimental feature or consulting deliverable with non-CITRIX hardware, software, services, data or other content or materials if such Infringement Claim would have been avoided by the use of the PRODUCT, experimental feature or consulting deliverable alone. THE FOREGOING STATES YOUR EXCLUSIVE REMEDY WITH RESPECT TO ANY INFRINGEMENT CLAIM OR ALLEGATION OF INFRINGEMENT. CITRIX assumes no liability, and shall have no liability, for any Infringement Claims or allegations of infringement based on: (i) your use of any PRODUCT, experimental feature or consulting deliverable after notice that you should cease use of such PRODUCT, experimental feature or consulting deliverable due to an Infringement Claim;;

5. LIMITED WARRANTY AND DISCLAIMER. CITRIX warrants that for a period of ninety (90) days from delivery of the License Keys, the software in a Software or Appliance PRODUCT will perform substantially in accordance with the PRODUCT's Documentation. Citrix warrants that for a period of one (1) year from delivery of the License Keys, the hardware in an Appliance PRODUCT, will be free from defects in material and workmanship in normal use. This hardware warranty does not cover any of the following: (i) improper installation, maintenance, adjustment, repair or modification by Customer or a third party; (ii) misuse, neglect, or any other cause other than ordinary use, including without limitation, accidents or acts of God;; (iii) improper environment, excessive or inadequate heating or air conditioning, electrical power failures, surges, water damage or other irregularities; (iv) third party software or software drivers; or (v) damage to hardware during shipment of an Appliance PRODUCT. CITRIX and its licensors and suppliers (SUPPLIERS) entire liability and your exclusive remedy under this software or hardware warranty (which is subject to your return of the PRODUCT to CITRIX or an authorized reseller) will be, at the sole option of CITRIX and subject to applicable law, to replace the PRODUCT or to refund the purchase price and terminate your license to any software on the PRODUCT. CITRIX assumes no liability, and shall have no liability, for any Infringement Claims or allegations of infringement based on: (i) your use of any PRODUCT, experimental feature or consulting deliverable after notice that you should cease use of such PRODUCT, experimental feature or consulting deliverable due to an Infringement Claim; (ii) any modification of the PRODUCT, experimental feature or consulting deliverable by you or at your direction; (iii) your combination of the PRODUCT, experimental feature or consulting deliverable with non-CITRIX hardware, software, services, data or other content or materials if such Infringement Claim would have been avoided by the use of the PRODUCT, experimental feature or consulting deliverable alone. THE FOREGOING STATES YOUR EXCLUSIVE REMEDY WITH RESPECT TO ANY INFRINGEMENT CLAIM OR ALLEGATION OF INFRINGEMENT '

6. DATA PROTECTION AND GDPR COMPLIANCE. Citrix agrees to deal with personal data relevant to Customers end-users in accordance with applicable data protection laws and regulations and the following: (a) with respect to personal data provided in connection with sales and marketing activities or use of Citrix websites, the Citrix Privacy Policy at <https://www.citrix.com/about/legal/privacy/>; (b) with respect to any personal information of European Union residents processed in connection with services, the Data Processing Agreement at <https://www.citrix.com/buy/licensing/citrix-data-processing-agreement.html> (European Union General Data Protection Regulation Terms); and (c) with respect to services, the Citrix Services Security Exhibit at <https://www.citrix.com/buy/licensing/citrix-services-security-exhibit.html>. Customer agrees to provide any notices and obtain any consent necessary for Citrix to access and process personal and other data as specified in this Agreement. The Privacy Policy, the Data Processing Agreement and the Citrix Services Security Exhibit are incorporated herein by reference.'

7. EXPORT RESTRICTION. You agree that you will not export, re-export, or import the PRODUCT, MAINTENANCE or any other software or service delivered hereunder in any form without the appropriate government licenses. You understand that under no circumstances may the PRODUCT, MAINTENANCE or any other software or service delivered hereunder be exported to: (i) any country subject to U.S. embargo, (ii) U.S.-designated denied persons or prohibited entities, or (iii) U.S. specially designated nationals

8. LIMITATION OF LIABILITY. EXCEPT FOR CITRIX' INDEMNIFICATION OBLIGATIONS EXPRESSLY SET FORTH IN SECTION 4, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, YOU AGREE THAT NEITHER CITRIX NOR ITS AFFILIATES, SUPPLIERS, OR AUTHORIZED DISTRIBUTORS SHALL BE LIABLE FOR ANY LOSS OF DATA OR PRIVACY, LOSS OF INCOME, LOSS OF OPPORTUNITY OR PROFITS, COST OF RECOVERY, LOSS, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, ARISING FROM YOUR USE OF THE PRODUCT, EXPERIMENTAL FEATURES, EVALUATION PRODUCT, MAINTENANCE OR ANY OTHER SOFTWARE OR SERVICE DELIVERED HEREUNDER, OR DAMAGE ARISING FROM YOUR USE OF THIRD PARTY PRODUCTS OR HARDWARE, OR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, OR YOUR EXPORTATION, REEXPORTATION, OR IMPORTATION OF ANY OR ALL OF THE SAME 'THIS LIMITATION WILL APPLY EVEN IF CITRIX,

ITS AFFILIATES, SUPPLIERS, OR AUTHORIZED DISTRIBUTORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN. EXCEPT FOR CITRIX INDEMNIFICATION OBLIGATIONS EXPRESSLY SET FORTH IN SECTION 4 (UNLESS NOTED AT <https://www.citrix.com/buy/licensing/product.html>), AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE TOTAL AGGREGATE LIABILITY OF CITRIX, ITS AFFILIATES, SUPPLIERS, OR AUTHORIZED DISTRIBUTORS EXCEED THE AMOUNT PAID FOR THE PRODUCT, MAINTENANCE TERM, CONSULTING DELIVERABLE OR ANY OTHER SOFTWARE OR SERVICE DELIVERED HEREUNDER AT ISSUE. TOTAL AGGREGATE LIABILITY IS LIMITED TO \$100.00US FOR ANY EXPERIMENTAL FEATURES OR ANY EVALUATION PRODUCT. ' 'YOU ACKNOWLEDGE THAT THE PRODUCT AND MAINTENANCE FEES REFLECT THESE ALLOCATIONS OF RISK. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. For purposes of this AGREEMENT, the term ;AFFILIATE; shall mean any entity that controls, is under common control with, or is controlled by CITRIX, where ;control; means the ownership, direct or indirect, of a majority of CITRIX stock or other interest entitled allowing the owner to direct the affairs of CITRIX. AFFILIATES, suppliers, and authorized distributors are intended to be third party beneficiaries of this AGREEMENT.'

9. TERMINATION AND SURVIVAL. This AGREEMENT is effective until terminated. You may terminate this AGREEMENT at any time by removing the software of your Software PRODUCT(s) from your computers and destroying all copies, and by removing the software of your Appliance PRODUCT(s) from the hardware, and then providing written notice to CITRIX with the serial numbers of your License Keys. CITRIX may terminate this AGREEMENT at any time for your breach of this AGREEMENT. Unauthorized copying of the software in a Software or Appliance PRODUCT or the Documentation or otherwise failing to comply with the license grant or restrictions of this AGREEMENT will result in automatic termination of this AGREEMENT and will make available to CITRIX all other legal remedies; You agree and acknowledge that your material breach of this AGREEMENT shall cause CITRIX irreparable harm for which monetary damages alone would be inadequate and that, to the extent permitted by applicable law, CITRIX shall be entitled to injunctive or equitable relief without the need for posting a bond. Upon termination of this AGREEMENT, the PRODUCT licenses granted hereunder will terminate and you must immediately destroy the software in a Software or Appliance PRODUCT and the Documentation, and all backup copies thereof. Any termination of consulting services is subject to the applicable scope definition, and you shall pay for services provided prior to the termination. All purchases are final with no right of return, and neither CITRIX nor any reseller or distributor will be obligated to pay, nor will you be due, any refund of amounts paid by you, other than under the Limited Warranty or Infringement Indemnification terms of this AGREEMENT. All purchases are subject to applicable taxes; Those provisions of this AGREEMENT, which are intended by the parties to survive, shall survive termination of this AGREEMENT, including without limitation, the Limitation of Liability terms '

10. U.S. GOVERNMENT END-USERS. If you are a U.S. Government agency, you hereby acknowledge and agree that the software in a Software or Appliance PRODUCT constitutes ;Commercial Computer Software; as defined in Section 2.101 of the Federal Acquisition Regulation (;FAR;), 48 CFR 2.101. Therefore, in accordance with Section 12.212 of the FAR (48 CFR 12.212), and Sections 227.7202-1 and 227.7202-3 of the Defense Federal Acquisition Regulation Supplement (;DFARS;) (48 CFR 227.7202-1 and 227.7202-3), the use, duplication, and disclosure of the software and related Documentation by the U.S. Government or any of its agencies is governed by, and is subject to, all of the terms, conditions, restrictions, and limitations set forth in this standard commercial license AGREEMENT.'; If, for any reason, FAR 12.212 or DFARS 227.7202-1 or 227.7202-3 or these license terms are deemed not applicable, you hereby acknowledge that the Government's right to use, duplicate, or disclose the software and related Documentation are 'Restricted Rights' as defined in 48 CFR Section 52.227-14(a) (May 2014) or DFARS 252.227-7014(a)(15) (Feb 2014), as applicable. Manufacturer is Citrix Systems, Inc., 851 West Cypress Creek Road, Fort Lauderdale, Florida 33309

11. AUTHORIZED DISTRIBUTORS AND RESELLERS. CITRIX authorized distributors and resellers do not have the right to make modifications to this AGREEMENT or to make any additional representations, commitments, or warranties binding on CITRIX

12. CHOICE OF LAW AND VENUE. The location of your providing entity will determine the choice of law and venue as identified at <https://www.citrix.com/buy/licensing/citrix-providing-entities.html>. If any provision of this AGREEMENT is invalid or unenforceable under applicable law, it shall be to that extent be deemed omitted and the remaining provisions will continue in full force and effect. To the extent a provision is deemed omitted, the parties agree to comply with the remaining terms of this AGREEMENT in a manner consistent with the original intent of the AGREEMENT. No waiver is effective unless signed by the party to be bound

13. ASSIGNMENT AND SUBCONTRACTING. Neither party hereto may assign this AGREEMENT, or any rights or obligations under it except as permitted by law or as set forth below, without the prior written consent of the other party, unless assigned to a successor in interest, or pursuant to a merger, corporate reorganization, or a sale or transfer of all or substantially all of the party's assets. You shall provide notice to CITRIX upon completion of any permitted assignment. In addition, you may assign this AGREEMENT to a majority-owned affiliate, and CITRIX may assign this AGREEMENT, or any rights or obligations under it to any AFFILIATE or any third party acquiring or otherwise assuming part of the business of CITRIX or any of its AFFILIATES. Subject to this restriction, this AGREEMENT will be binding upon and inure to the benefit of the parties hereto, their successors and assigns. CITRIX may use subcontractors to provide services to you under this AGREEMENT, but CITRIX shall remain responsible to you for the performance of the services

14. FORCE MAJEURE. CITRIX and/or any of its AFFILIATES shall not be liable for any delay or failure to perform any obligation under this AGREEMENT where the delay or failure results from any cause beyond its/their reasonable control, including without limitation: (i) acts of God; (ii) electrical power failures or surges; (iii) utilities or other telecommunications failures; (iv) storms or other elements of nature; or (v) terrorism or acts of war; but only for so long as such condition exists

15. HOW TO CONTACT CITRIX. Should you have any questions concerning this AGREEMENT or want to contact CITRIX for any reason, write to CITRIX Customer Service at the address identified at <https://www.citrix.com/buy/licensing/citrix-providing-entities.html>;

16. TRADEMARKS. This AGREEMENT does not grant you the right to use any CITRIX trade or service mark. For information about proper permitted usage of CITRIX trademarks please see: <http://www.citrix.com/about/legal/brand-guidelines.html>;

# Microsoft Software License Terms

Terms and conditions for using Microsoft software, including Windows IoT Enterprise.

Updated April 2024

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS IOT ENTERPRISE (ALL EDITIONS)

IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 8. IT AFFECTS HOW DISPUTES ARE RESOLVED.

Thank you for choosing Microsoft. Depending on how you obtained the Windows software, this is a license agreement between (i) you and the device manufacturer or software installer that distributes the software with your device; or (ii) you and Microsoft Corporation (or, based on where you live or, if a business, where your principal place of business is located, one of its affiliates) if you acquired the software from a retailer. Microsoft is the device manufacturer for devices that are produced by Microsoft or one of its affiliates, and Microsoft is the retailer if you acquired the software directly from Microsoft. If you are a volume license customer, use of this software is subject to your volume license agreement rather than this agreement. This agreement describes your rights, obligations, and the conditions upon which you may use the Windows software. You should review the entire agreement, including any supplemental license terms that accompany the software and any linked terms, because all the terms are important and together create this agreement that applies to you. You can review linked terms by pasting the (aka.ms/) link into a browser window. By accepting this agreement or using the software, you agree to all these terms, and consent to the transmission of certain information during activation and during your use of the software as per the privacy statement described in Section 3. If you do not accept and comply with these terms, you may not use the software or its features. You may contact the device manufacturer or installer, or your retailer if you purchased the software directly, to determine its return policy and return the software or device for a refund or credit under that policy. You must comply with that policy, which might require you to return the software with the entire device on which the software is installed for a refund or credit, if any.

## 1. Overview

- a. **Applicability**—This agreement applies to the Windows software that is preinstalled on your device, or acquired from a retailer and installed by you, the media on which you received the software (if any), any fonts, icons, images, or sound files included with the software, and also any Microsoft updates, upgrades, supplements or services for the software, unless other terms come with them. It also applies to Windows apps developed by Microsoft that provide functionality such as mail, calendar, contacts, music, and news that are included with Windows, unless other terms apply. If this agreement contains terms regarding a feature or service not available on your device, those terms do not apply.
- b. **Additional terms**—Additional Microsoft and third-party terms may apply to your use of certain features, services, and apps, depending on your device's capabilities, how it is configured, and how you use it. Please read them.
  - i. Some Windows apps provide an access point to, or rely on, online services, and the use of those services is sometimes governed by separate terms and privacy policies, such as the Microsoft Services Agreement at <https://aka.ms/msa>. You can view these terms and policies by looking at the service terms of use or the app's settings, as applicable; please read them. The services may not be available in all regions.
  - ii. Microsoft, or the device manufacturer or installer may include additional apps, which will be subject to separate license terms and privacy policies.
  - iii. The software may include third-party programs that are licensed to you under this agreement, or under their own terms. License terms, notices, and acknowledgments, if any, for the third-party programs can be viewed at C:\Windows\Help\en-US\credits.rtf.

## 2. Installation and Use Rights

- a. **License**—The software is licensed, not sold. The software license is permanently assigned to the device with which you acquired the software. Under this agreement, we grant you the right to install and run one instance of the software on your device (the licensed device), so long as you comply with the terms and restrictions that are contained in this agreement. Updating or upgrading from non-genuine software with software from Microsoft or authorized sources does not make your original version or the updated/upgraded version genuine, and in that situation, you do not have a license to use the software.
- b. **Device**—In this agreement, "device" means a physical hardware system with an internal storage device capable of running the software, or a virtual machine. A hardware partition or blade is considered to be a device.
- c. **Restrictions**—

- i. Use or virtualized features of the software separately;
- ii. Publish, copy (other than the permitted backup copy), rent, lease, or lend the software;
- iii. Transfer the software (except as permitted by this agreement);
- iv. Work around any technical restrictions or limitations in the software;
- v. Use the software as server software or to operate the device as a server, except as permitted under Section 2(d)(iii) below; use the software to offer commercial hosting services; make the software available for simultaneous use by more than one user over a network, except as permitted under Section 2(d)(vi) below; install the software on a server for remote access or use over a network; or install the software on a device for use only by remote users; a single device may be locally and simultaneously interacted with by up-to two end user operators;
- vi. Reverse engineer, decompile, or disassemble the software, or attempt to do so, except and only to the extent that the foregoing restriction is (a) permitted by applicable law; (b) permitted by licensing terms governing the use of open-source components that may be included with the software; or (c) required to debug changes to any libraries licensed under the GNU Lesser General Public License that are included with and linked to by the software;
- vii. When using Internet-based features you may not use those features in any way that could interfere with anyone else's use of them.

**d. Multi-Use scenarios—**

- Multiple versions. If when acquiring the software, you were provided with multiple versions (such as 32-bit and 64-bit versions), you may install and activate only one of those versions at a time.
- Multiple or pooled connections. Hardware or software you use to multiplex or pool connections, or reduce the number of devices or users that access or use the software, does not reduce the number of licenses you need. You may only use such hardware or software if you have a license for each instance of the software you are using.
- Device connections. You may allow up to 20 other devices to access the software installed on the licensed device solely to use the following software features for personal or internal purposes: file services, print services, Internet information services, and Internet connection sharing and telephony services on the licensed device. The 20 connection limit applies to devices that access the software indirectly through "multiplexing" or other software or hardware that pools connections. You may allow any number of devices to access the software on the licensed device to synchronize data between devices. This subsection does not mean, however, that you have the right to install the software, or use the primary function of the software (other than the features listed in this subsection), on any of these other devices.
- Remote access. Users may access the licensed device from another device using remote access technologies, but only on devices separately licensed to run the same or higher edition of this software.
- Remote assistance. You may use remote assistance technologies to share an active session without obtaining any additional licenses for the software. Remote assistance allows one user to connect directly to another user's computer, usually to correct problems.
- POS application. If the software is installed on a retail point of service device, you may use the software with a point of service application ("POS Application"). A POS Application is a software application which provides only the following functions: (i) process sales and service transactions, scan and track inventory, record and/or transmit customer information, and perform related management functions, and/or (ii) provide information directly and indirectly to customers about available products and services. You may use other programs with the software as long as the other programs: (i) directly support the manufacturer's specific use for the device, or (ii) provide system utilities, resource management, or anti-virus or similar protection. For clarification purposes, an automated teller machine ("ATM") is not a retail point of service device.
- Cloud Computing Devices. If your device uses Internet browsing functionality to connect to and access cloud hosted applications: (i) no desktop functions may run locally on the device, and (ii) any files that result from the use of the desktop functions may not be permanently stored on the system. "Desktop functions," as used in this agreement, means a consumer or business task or process performed by a computer or computing device. This includes but is not limited to email, word processing, spreadsheets, database, scheduling, network or internet browsing and personal finance.
- Desktop Functions. If your system performs desktop functions, then you must ensure that they: (i) are only used to support the application, and (ii) operate only when used with the application.

**e. Specific Use—**The manufacturer designed the licensed device for a specific use. You may only use the software for that use.

**f. High Risk Use—**

- i. **WARNING: THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE WHERE FAILURE OR FAULT OF ANY KIND OF THE SOFTWARE COULD RESULT IN DEATH OR SERIOUS BODILY INJURY, OR IN PHYSICAL OR ENVIRONMENTAL DAMAGE** (collectively "High Risk Use"). Accordingly, You must design and implement Your hardware and software such that, in the event of any interruption, defect, error, or other failure of the software, the safety of people, property, and the environment are not reduced below a level that is reasonable, appropriate, and legal, whether in general or for a specific industry. Your High Risk Use of the software is at Your own risk.
- ii. **Indemnification.** You agree to indemnify, defend and hold harmless Microsoft from any claims, including claims arising from any High Risk Uses, and inclusive of attorneys' fees, related to the distribution or use of Your devices, except to the extent that any intellectual property claim is based solely on the unmodified software.

3. **Privacy; Consent to Use of Data**—Your privacy is important to us. Some of the software features send or receive information when using those features. Many of these features can be switched off in the user interface, or you can choose not to use them. By accepting this agreement and using the software you agree that Microsoft may collect, use, and disclose the information as described in the Microsoft Privacy Statement available at <https://aka.ms/privacy>, and as may be described in the user interface associated with the software features.
4. **Authorized Software and Activation**—You are authorized to use this software only if you are properly licensed and the software has been properly activated with a genuine product key or by other authorized method. When you connect to the Internet while using the software, the software will automatically contact Microsoft or its affiliate to confirm the software is genuine and the license is associated with the licensed device. You can also activate the software manually by Internet or telephone. In either case, transmission of certain information will occur, and Internet, telephone and SMS service charges may apply. During activation (or reactivation that may be triggered by changes to your device's components), the software may determine that the installed instance of the software is counterfeit, improperly licensed or includes unauthorized changes. If activation fails the software will attempt to repair itself by replacing any tampered Microsoft software with genuine Microsoft software. You may also receive reminders to obtain a proper license for the software. Successful activation does not confirm that the software is genuine or properly licensed. You may not bypass or circumvent activation. To help determine if your software is genuine and whether you are properly licensed, see <https://aka.ms/genuine>. Certain updates, support, and other services might be offered only to users of genuine Microsoft software.
5. **Updates**—The software periodically checks for system and app updates, and may download and install them for you. You may obtain updates only from Microsoft or authorized sources, and Microsoft may need to update your system to provide you with those updates. To the extent automatic updates are enabled on your device, by accepting this agreement, or using the software, you agree to receive these types of automatic updates without any additional notice.
6. **Geographic and Export Restrictions**—If your software is restricted for use in a particular geographic region, then you may activate the software only in that region. You must also comply with all domestic and international export laws and regulations that apply to the software, which include restrictions on destinations, end users, and end use. For further information on geographic and export restrictions, visit <https://aka.ms/exporting>.
7. **Device Manufacturer and Installer Support and Refund Procedures**—For the software generally, contact the device manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft may provide limited support services for properly licensed software as described at <https://aka.ms/mssupport>. If you are seeking a refund, contact the device manufacturer or installer to determine its refund policies. You must comply with those policies, which might require you to return the software with the entire device on which the software is installed for a refund.
8. **Binding Arbitration and Class Action Waiver if You Live in (or, if a Business, Your Principal Place of Business is in) the United States**—We hope we never have a dispute, but if we do, you and we agree to try for 60 days, upon receipt of a Notice of Dispute, to resolve it informally. If we can't, you and we agree to binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury. Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of appeal under the FAA. Class action lawsuits, class-wide arbitrations, private attorney-general actions, request for public injunctions, and any other proceeding or request for relief where someone acts in a representative capacity aren't allowed. Nor is combining individual proceedings without the consent of all parties. "We," "our," and "us" includes Microsoft, the device manufacturer, software installer, and our affiliates.
- a. **Disputes covered—everything except IP.** The term "dispute" is as broad as it can be. It includes any claim or controversy between you and the device manufacturer or installer, or you and Microsoft, concerning the software (or software to which this agreement applies including other Windows apps), its price, marketing, communications, your purchase transaction, billing, or this agreement, under any legal theory including contract, warranty, tort, statute, or regulation, except disputes relating to the enforcement or validity of your, your licensors', our, or our licensors' intellectual property rights.
- b. **Send a Notice of Dispute before arbitration.** If you have a dispute that our customer service representatives can't resolve and you wish to pursue arbitration, you must first send an individualized Notice of Dispute by U.S. Mail to the device manufacturer or installer, ATTN: LEGAL DEPARTMENT. If your dispute is with Microsoft, you must first mail it to Microsoft Corporation, ATTN: CELA ARBITRATION, One Microsoft Way, Redmond, WA 98052-6399, or submit the form electronically. The Notice of Dispute form is available at <https://go.microsoft.com/fwlink/?LinkId=245499>. Complete that form in full, with all the information it requires. We'll do the same if we have a dispute with you. Any applicable statute of limitations will be tolled from the date of a properly submitted individualized Notice of Dispute through the first date on which an arbitration may properly be filed under this Section 8.
- c. **Small claims court option.** Instead of sending a Notice of Dispute, either you or we may sue the other party in small claims court seeking only individualized relief, so long as the action meets the small claims court's requirements and remains an individual action seeking individualized relief. The small claims court must be in your county of residence (or, if a business, your principal place of business).
- d. **Arbitration procedure.** The AAA will conduct any arbitration under its Commercial Arbitration Rules (or if you are an individual and use the software for personal or household use, or if the value of the dispute is less than \$75,000 USD whether or not you are an individual or how you use the software, its Consumer Arbitration Rules). For more information, see <https://aka.ms/adr>. This agreement governs to the extent it conflicts with any applicable AAA rules. To initiate an arbitration, submit the Demand for Arbitration form available at <https://go.microsoft.com/fwlink/?LinkId=245497> to the

AAA and mail a copy to the device manufacturer or installer (or to Microsoft if your dispute is with Microsoft). The form must contain information that is specific to you and your claim. In a dispute involving \$25,000 USD or less, any hearing will be telephonic or by videoconference unless the arbitrator finds good cause to hold an in-person hearing instead. Any in-person hearing will take place in your county of residence (or, if a business, your principal place of business). The arbitrator may award the same damages to you individually as a court could. The arbitrator may award declaratory or injunctive relief only to you individually to satisfy your individual claim, but not relief that would affect non-parties. The arbitrator rules on all issues except that a court has exclusive authority: (i) to decide arbitrability, as well as formation, existence, scope, validity, and enforceability of this arbitration agreement; (ii) to decide whether the parties have complied with the pre-arbitration requirements (including the individualized Notice of Dispute and Demand for Arbitration forms); (iii) to enforce the prohibition on class, representative, private attorney-general, or combined actions or proceedings, or public injunctive relief; and (iv) to enjoin an arbitration from proceeding if it does not comply with this agreement. If your Notice of Dispute involves claims similar to those of at least 24 other customers, and if you and those other customers are represented by the same lawyers, or by lawyers who are coordinating with each other, you and we agree that these claims will be “Related Cases.” Related Cases may only be filed in batches of up to 50 individual arbitrations at a time, and those individual arbitrations will be resolved in the following manner: (i) for the first batch, each side may select up to 25 of these Related Cases to be filed and resolved in individual arbitrations under this Section 8; (ii) none of the other Related Cases may be filed or prosecuted in arbitration until the first batch of up to 50 individual arbitrations is resolved; and (iii) if, after that first batch, the parties are unable to informally resolve the remaining Related Cases, a second batch of Related Cases may be filed, where each side may select up to 25 of the Related Cases to be resolved in individual arbitrations under this Section 8. This process of batched individual arbitrations will continue until the parties resolve all Related Cases informally or through individual arbitrations. A court has exclusive authority to enforce this paragraph, including whether it applies to a given set of claims, and to enjoin the filing or prosecution of arbitrations that do not comply with this paragraph.

**e. Arbitration fees and payments—**

- i. Disputes involving less than \$75,000 USD. The device manufacturer or installer (or Microsoft if your dispute is with Microsoft) will promptly reimburse your filing fees and pay the AAA’s and arbitrator’s fees and expenses. If (i) the dispute involves less than \$75,000 USD; and before initiating arbitration (ii) you complied with all pre-arbitration requirements in this Section 8, including, if applicable, the Related Cases paragraph. Otherwise, the AAA rules will govern payment of filing fees and the AAA’s and arbitrator’s fees and expenses. If, at the conclusion of the arbitration, the arbitrator awards you more than our last written offer made before the arbitrator was appointed, the device manufacturer or installer (or Microsoft if your dispute is with Microsoft) will pay you: (i) the amount of the award or \$1,000 USD (whichever is more); (ii) any reasonable attorney’s fees you incurred; and (iii) any reasonable expenses (including expert witness fees and costs) that your attorney accrued in connection with your individual arbitration.
- ii. Disputes involving \$75,000 USD or more. The AAA rules will govern payment of filing fees and the AAA’s and arbitrator’s fees and expenses.

**f. Severability—**If, after exhaustion of all appeals, a court finds any part of this Section 8 unenforceable as to any claim or request for a remedy, then the parties agree to arbitrate all claims and remedies subject to arbitration before litigating in court any remaining claims or remedies (such as a request for a public injunction remedy, in which case the arbitrator issues an award on liability and individual relief before a court considers that request). Otherwise, if any other part of Section 8 is found to be unenforceable, the remainder will remain in effect (with an arbitration award issued before any court proceeding begins).

**g. Microsoft as party or third-party beneficiary—**If Microsoft is the device manufacturer or if you acquired the software from a retailer, Microsoft is a party to this agreement. Otherwise, Microsoft is not a party but is a third-party beneficiary of your agreement with the device manufacturer or installer to resolve disputes through informal negotiation and arbitration.

**9. Governing Law—**The laws of the state or country where you live (or, if a business, where your principal place of business is located) govern all claims and disputes concerning the software, its price, or this agreement, including breach of contract claims and claims under state consumer protection laws, unfair competition laws, implied warranty laws, for unjust enrichment, and in tort, regardless of conflict of law principles. In the United States, the FAA governs all provisions relating to arbitration.

**10. Consumer Rights, Regional Variations—** This agreement describes certain legal rights. You may have other rights, including consumer rights, under the laws of your state or country. You may also have rights with respect to the party from which you acquired the software. This agreement does not change those other rights if the laws of your state or country do not permit it to do so. For example, if you acquired the software in one of the below regions, or mandatory country law applies, then the following provisions apply to you:

**a. Australia—**References to “Limited Warranty” are references to the express warranty provided by Microsoft or the device manufacturer or installer. This warranty is given in addition to other rights and remedies you may have under law, including your rights and remedies under the Australian Consumer Law consumer guarantees. Nothing in this agreement limits or changes those rights and remedies. In particular: (i) support and refund policies referred to in Section 7 are subject to the Australian Consumer Law; (ii) the Australian Consumer Law consumer guarantees apply to the evaluation software described in Section 11(d)(i); and (iii) our goods come with guarantees that cannot be excluded under the Australian Consumer Law. In this subsection, “goods” refers to the software for which Microsoft, or the device



manufacturer or installer provides the express warranty. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. To learn more about your rights under the Australian Consumer Law, please review the information at <https://aka.ms/acl>.

b. **Canada**—You may stop receiving updates on your device by turning off Internet access. If and when you re-connect to the Internet, the software will resume checking for and installing updates.

c. **Germany and Austria**—

- i. **Warranty.** The properly licensed software will perform substantially as described in any Microsoft materials that accompany the software. However, the device manufacturer or installer, and Microsoft, give no contractual guarantee in relation to the licensed software.
- ii. **Limitation of Liability.** In case of intentional conduct, gross negligence, claims based on the Product Liability Act, as well as, in case of death or personal or physical injury, the device manufacturer or installer, or Microsoft is liable according to the statutory law. Subject to the preceding sentence, the device manufacturer or installer, or Microsoft will only be liable for slight negligence if the device manufacturer or installer or Microsoft is in breach of such material contractual obligations, the fulfillment of which facilitate the due performance of this agreement, the breach of which would endanger the purpose of this agreement and the compliance with which a party may constantly trust in (so-called "cardinal obligations"). In other cases of slight negligence, the device manufacturer or installer or Microsoft will not be liable for slight negligence.

d. **Other regions**—See <https://go.microsoft.com/fwlink/?LinkId=534978> for a current list of regional variations

## 11. Additional Notices —

a. **Networks, data and Internet usage**—Some features of the software and services accessed through the software may require your device to access the Internet. Your access and usage (including charges) may be subject to the terms of your cellular or internet provider agreement. Certain features of the software may help you access the Internet more efficiently, but the software's usage calculations may be different from your service provider's measurements. You are always responsible for (i) understanding and complying with the terms of your own plans and agreements, and (ii) any issues arising from using or accessing networks, including public/open networks. You may use the software to connect to networks, and to share access information about those networks, only if you have permission to do so.

b. **Codec Notices**—

- i. **H.264/AVC Video Standard.** This product includes AVC coding technology. MPEG LA LLC requires this notice:
  - i. This product is licensed under the AVC patent portfolio license for the personal and non-commercial use of a consumer to:
    - ~~Order List Number 5~~ Compliance with the AVC standard ("AVC VIDEO").
    - ~~Order List Number 5~~ that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed to provide AVC video.
  - ii. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA LLC. See <http://www.MPEGLA.COM>.
  - iii. For clarification purposes, this notice does not limit or inhibit the use of the product for normal business uses that are personal to that business which do not include:
    - ~~Order List Number 5~~ the product to third parties.
    - ~~Order List Number 5~~ with AVC Standard compliant technologies for distribution to third parties.
- ii. **VC-1 Video Standard.** This product includes VC-1 coding technology. MPEG LA LLC requires this notice:
  - i. This product is licensed under the VC-1 Patent Portfolio license for the personal and non-commercial use of a consumer to:
    - ~~Order List Number 5~~ Compliance with the VC-1 standard ("VC-1 Video").
    - ~~Order List Number 5~~ that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed to provide VC-1 video.
  - ii. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA LLC. See <http://www.MPEGLA.COM>.

For clarification purposes, this notice does not limit or inhibit the use of the product for normal business uses that are personal to that business which do not include (i) redistribution of the product to third parties, or (ii) creation of content with VC-1 Standard compliant technologies for distribution to third parties.

c. **Malware protection**—Microsoft cares about protecting your device from malware. The software will turn on malware protection if other protection is not installed or has expired. To do so, other antimalware software will be disabled or may have to be removed.

d. **Limited rights versions**—If the software version you acquired is marked or otherwise intended for a specific or limited use, then you may only use it as specified. You may not use such versions of the software for commercial, non-profit, or revenue-generating activities.

- i. **Evaluation**—For evaluation (or test or demonstration) use, you may not sell the software, use it in a live operating environment, or use it after the evaluation period. Notwithstanding anything to the contrary in this Agreement, evaluation software is provided "AS IS" and no warranty, implied or express (including the Limited Warranty), applies to these versions.

**12. Entire Agreement**—This agreement (together with the printed paper license terms or other terms accompanying any software supplements, updates, and services that are provided by the device manufacturer or installer, or Microsoft, and that you use), and the terms contained in web links listed in this agreement, are the entire agreement for the software and any such supplements, updates, and services (unless the device manufacturer or installer, or Microsoft, provides other terms with such supplements, updates, or services). You can review this agreement after your software is running by going to <https://aka.ms/useterms> or going to Settings - System - About within the software. You can also review the terms at any of the links in this agreement by typing the URLs into a browser address bar, and you agree to do so. You agree that you will read the terms before using the software or services, including any linked terms. You understand that by using the software and services, you ratify this agreement and the linked terms. There are also informational links in this agreement. The links containing notices and binding terms are:

- [Windows Privacy Statement](#)
- [Microsoft Services Agreement](#)