

Zebra Workstation Connect



ZEBRA

Administrator's Guide

2024/06/28

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2024 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/informationpolicy.

COPYRIGHTS: zebra.com/copyright.

PATENTS: ip.zebra.com.

WARRANTY: zebra.com/warranty.

END USER LICENSE AGREEMENT: zebra.com/eula.

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Contents

About This Guide.....	5
Configurations.....	5
Revision History.....	8
Supported Peripherals.....	10
Icon Conventions.....	10
Notational Conventions.....	11
Service Information.....	11
Zebra DNA Cloud.....	12
Configuring the Do Not Change Setting.....	14
Configuring the External Monitor Orientation.....	15
Configuring Display Settings.....	15
Configuring the External Monitor Resolution.....	16
Configuring External Monitor Density.....	17
Monitor Size.....	17
Screen Size (Inches).....	18
Desktop UI Elements.....	18
Configuring Freeform Windows.....	19
Configuring the Visibility of Status Icons.....	20
Sorting Desktop Shortcuts.....	21
Importing Shortcuts.....	21
Mass Deploying Shortcuts.....	22
Configuring the Desktop Home Screen Wallpaper.....	23
Using Immersive Mode.....	23
Configuring Application Behaviors.....	25

Configuring Device User Access.....	27
Configuring Screen Capture Permissions.....	28
Configuring the Desktop Soft Input Panel (SIP).....	28
Enabling or Disabling the All Applications Button.....	29
Configuring Device Behavior.....	29
Enabling Persistence.....	30
Resetting the Current Configuration.....	31
Update Behavior.....	31
Versioning.....	33
Using the Feedback Channel.....	33
Using Generic Intents.....	34
Editing the Name and Description of the Configuration.....	34
System Configuration Features.....	35
Preventing Automatic Application Updates.....	35
Keyboard Configuration.....	36
USB Scanner Configuration.....	37
Remote Control and Screen Share.....	37
Supporting Zebra Enterprise Applications.....	38
Configuring the Audio UI.....	39
Best Available Audio Output Paths.....	39
Optimizing User Access to Applications.....	40
Guidelines for Kiosk Behavior.....	42
MDNA Licensing.....	44
L10 Tablet Considerations.....	45
Version Support.....	45
Secure Mass Deployment of Managed Configurations.....	45
Lock-task Mode.....	45
Troubleshooting.....	47

About This Guide

This guide provides information about developing applications for Zebra Workstation Connect.

Configurations

This guide covers the following configurations:

Table 1 Compatible Configurations

Configuration	Description	Device Compatibility
CRD-EC5X-1SWS-01	<p>Workstation Docking Cradle Kit with Standard Cup, HDMI, Ethernet, and multiple USB Ports.</p> <p>Included in the kit:</p> <ul style="list-style-type: none">• Cradle (for example, CRD-EC5X-1SWS-02)• Power Supply (for example, PWRBGA12V50W0WW)• DC Cable (for example, CBL-DC-388A1-01) <p>Country-specific AC line cords are sold separately.</p>	EC50 and EC55 Mobile Computers

Table 1 Compatible Configurations (Continued)

Configuration	Description	Device Compatibility
CRD-TC2X-1SNWS-01	<p>The TC21, TC26, TC21-HC, TC26-HC Connect Cradle (Workstation) connects a mobile computer to an external monitor and multiple peripherals, including HDMI, Ethernet, USB-A (4), and a 3.5mm headset jack.</p> <p>Included in the kit:</p> <ul style="list-style-type: none"> • Cradle (for example, CRD-TC2X-1SNWS-01) • Power Supply (for example, PWR-BGA12V50W0WW) • DC Cable (for example, CBL-DC-388A2-01) <p>Country-specific AC line cords are sold separately.</p>	TC21, TC26, TC21-HC, and TC26-HC Mobile Computers
CRD-TC5X-1SWS-01	<p>Workstation Docking Cradle Kit with Standard Cup, HDMI, Ethernet, and multiple USB Ports.</p> <p>Included in the kit:</p> <ul style="list-style-type: none"> • Cradle (for example, (CRD-TC5X-1SWS1-01) • Power Supply (for example, PWRBGA12V50W0WW) • DC Cable (for example, CBL-DC-388A1-01) <p>Country-specific AC line cords are sold separately.</p>	TC52, TC52x, TC57, TC57x, TC52ax, TC52x-HC and TC52ax-HC Mobile Computers
CRD-NTC5X-1SNWS-01	<p>The TC53, TC58 Connect Cradle (Workstation) connects a mobile computer to an external monitor and multiple peripherals, including HDMI, Ethernet, and USB-A (4)</p> <p>Included in the kit:</p> <ul style="list-style-type: none"> • Cradle (for example, CRD-NTC5X-1SNWS-01) • Power Supply (for example, PWR-BGA12V50W0WW) • DC Line Cord (for example, CBL-DC-388A2-01) <p>Country-specific grounded AC Line Cord sold separately.</p>	TC53 and TC58 Mobile Computers

Table 1 Compatible Configurations (Continued)

Configuration	Description	Device Compatibility
CRD-NTC7X-1SNWS-01	<p>The TC73/TC78 Connect Cradle (Workstation) connects a mobile computer to an external monitor and multiple peripherals, including HDMI, Ethernet, and USB-A (4).</p> <p>Included in the kit:</p> <ul style="list-style-type: none"> • Cradle (for example, CRD-NTC7X-1SNWS-01) • Power Supply (for example, PWR-BGA12V50W0WW) • DC Line Cord (for example, CBL-DC-388A2-01) <p>Country-specific AC line cords are sold separately.</p>	TC73 and TC78 Mobile Computers
CRD-ET4X-1SNWS-01	<p>The ET40, ET45, ET40-HC, ET45-HC Connect Cradle (Workstation) connects a 10 or 8 in. tablet to an external monitor and multiple peripherals, including HDMI, Ethernet, USB-A (x4), and a 3.5 mm headset jack.</p> <p>Included in the kit:</p> <ul style="list-style-type: none"> • Cradle (for example, CRD-ET4X-1SNWS-01) • Power Supply (for example, PWR-BGA12V50W0WW) • DC Line Cord (CBL-DC-388A2-01) <p>Country-specific grounded AC Line Cord sold separately.</p>	ET40, ET45, ET40-HC, ET45-HC Tablets

Table 1 Compatible Configurations (Continued)

Configuration	Description	Device Compatibility
CRD-ET5X-1SWS-01	<p>Workstation Docking Cradle Kit with Standard Cup, HDMI, Ethernet, and multiple USB Ports.</p> <p>Included in the kit:</p> <ul style="list-style-type: none"> • Cradle with Rugged I/O Adaptor (for example, CRD-ET5X-1SCOM2R) • Cradle (for example, CRD-ET5X-1SCOM1) • Power Supply (for example, PWRBGA12V50W0WW) • DC Cable (for example, CBL-DC-388A1-01) <p>Country-specific AC line cords are sold separately.</p>	ET51 and ET56 Mobile Computers
CRD-L10A-XVEHCOMS21-01	The L10 tablet comes with a Lithium-ion battery and a power supply.	L10 Tablets



NOTE: A Mobility DNA Enterprise license is required to use Zebra Workstation Connect on Zebra Professional series devices.

Revision History

The following table describes the changes made for each revision.

Revision	Date	Description	Zebra Workstation Connect Version
-11 Rev. A	6/30	<p>Updates in this version include:</p> <ul style="list-style-type: none"> • Support for Lock-task Mode 	3.1
-10 Rev. A	3/24	<p>Updates in this version include:</p> <ul style="list-style-type: none"> • Support for Android 13 	3.0
-09 Rev. A	10/23	<p>Updates in this version include:</p> <ul style="list-style-type: none"> • Secure Mass Deployment of configuration files (instead of using managed configurations) • Enable Do Not Change to configure a subset of settings 	2.0
-08 Rev A	2/23	<p>Updates in this version include:</p> <ul style="list-style-type: none"> • Immersive Mode 	1.7

About This Guide

Revision	Date	Description	Zebra Workstation Connect Version
		<ul style="list-style-type: none"> • Display Settings 	
-07 Rev A	12/22	Updates in this version include: <ul style="list-style-type: none"> • Screen Resolution (Inches) • Version Control • Always Docked Mode • Paste Shortcuts from the Clipboard • Licensing 	1.6
-06 Rev A	8/22	Updates in this version include: <ul style="list-style-type: none"> • New Scanner Support • Configuration Reset Enable/Disable • Custom Shortcut Icons Enable/Disable • Troubleshooting 	1.5
-05 Rev A	5/22	Updates in this version include: <ul style="list-style-type: none"> • Desktop UI Elements • Freeform Windows • Desktop SIP Configuration • Application Behavior Persistence 	1.4
-04 Rev A	3/22	Updates in this version include: <ul style="list-style-type: none"> • System Configurations • Remote Control 	1.3
-03 Rev A	12/21	Updates in this version include: <ul style="list-style-type: none"> • Screen Sharing/Remote Control. • EMM Lockdown • Audio Settings • Screen Density • Screen Capture • Restrict Mobile Application Taskbar Access at the Package Level. • Screen Dimming 	1.2

Revision	Date	Description	Zebra Workstation Connect Version
-02 Rev A	10/21	<p>Updates in this version include:</p> <ul style="list-style-type: none"> • Advanced Application Permissions on the Desktop Home Screen. • Enable or Disable the All Apps Button on the Desktop Taskbar. • Enable or Disable Mobile Device Application Icons on the Desktop Taskbar. • Access to Device Settings from the Taskbar Status Icons. • Soft Input Panel (SIP) Taskbar Icon. • Configuration of the External Keyboard Layout. • DS9308 USB Scanner Support (ET56 only). 	1.1
-01 Rev A	8/21	Initial Release	1.0

Supported Peripherals

Peripherals supported by the Zebra Workstation Cradle include:

- External touch and non-touch HDMI monitor.
- USB-A Keyboard
- USB-A Mouse
- USB-A Headsets and Headphones
- Zebra External Scanners (connected via USB-A):
 - DS9308, DS9908, DS8108, DS4608, DS2208, DS2278, DS3678-SR, DS3608-SR, DS9308-SR, and MP7000 (scanning available Zebra USB scanners only, scaling available on 6490 platform devices running Android 11). For additional information on Zebra platform devices, go to supportcommunity.zebra.com/s/article/000022440.



NOTE: For ET5X tablets, headsets can be connected via the USB-C port on the tablet. USB-A headsets or headphones connected to the USB-A ports of the communication cradle are not supported.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.



NOTE: The text here indicates information that is supplemental for the user to know and that is not required to complete a task.



IMPORTANT: The text here indicates information that is important for the user to know.



CAUTION: If the precaution is not heeded, the user could receive a minor or moderate injury.



WARNING: If danger is not avoided, the user CAN be seriously injured or killed.



DANGER: If danger is not avoided, the user WILL be seriously injured or killed.

Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
 - Dialog box, window, and screen names
 - Dropdown list and list box names
 - Checkbox and radio button names
 - Icons on a screen
 - Key names on a keypad
 - Button names on a screen
- Bullets (•) indicate:
 - Action items
 - List of alternatives
 - Lists of required steps that are not necessarily sequential.
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

Service Information

If you have a problem with your equipment, contact Zebra Global Customer Support for your region. Contact information is available at: zebra.com/support.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number

Zebra responds to calls by email, telephone, or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Customer Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your Zebra business product from a Zebra business partner, contact that business partner for support.

Zebra DNA Cloud

Before attempting the tasks described in this section, ensure that your organization has set up Zebra DNA Cloud. After one or more devices are enrolled and licensed in the Zebra DNA Cloud system, you can create and deploy device configurations or perform other administrative tasks such as email communication or document creation.

The My Apps section is for installing apps on devices and deploying related files. Apps are uploaded to the Zebra DNA Cloud system in a Collection, after which the administrator creates an App Setup Profile, designating an APK (selected from the Collection) for deployment along with configuration and data file(s)

Zebra DNA Cloud stores applications in Collections. Applications preinstalled on Zebra devices are viewable in the **Zebra Collection** tab. Applications installed by an organization are viewable in the My Collection tab.

The section below presents the screenshots for installing and configuring Zebra Workstation Connect using Zebra DNA Cloud.

The screenshot displays the Zebra DNA Cloud interface. On the left is a navigation sidebar with options: Dashboard, New Device Setup, My Devices, Device Settings, My Apps (highlighted), Android Updates, and Licensing. The main area is titled 'My Apps' and includes a sub-header 'App setup and configuration page. Zebra recommends testing all app configurations on a small group of dissimilar devices before broadly deploying to an enterprise.' Below this are three tabs: 'Zebra Collection' (selected), 'My Collection', and 'App Setup'. A 'New Setup' button is in the top right. The main content is a grid of application cards, each with a description, version dropdown, and 'Setup' button. The 'Workstation Connect' card is highlighted. Other cards include 'Device Diagnostics Tool', 'Enterprise Browser', 'Enterprise Home Screen', 'Enterprise Keyboard', and 'Device Central'.

1. On the Zebra Collection tab, click **Setup** next to Workstation Connect to set up the application.

2. On the **App Details** page, confirm the information, and click **Next** to proceed.

Create New App Setup

1 Select App

2 Configure App

3 Name and Description

4 Review and Apply

Select an App from

Zebra Collection

App Name: App Version:

For Android version compatibility info, visit Zebra Collection.

My Collection

App Name: App Version: Add App

App Details

APP NAME	HOSTING LOCATION	APP VERSION	DEVELOPER	PACKAGE NAME	APP DESCRIPTION

Discard Next

3. Select **Yes** to edit and include the configuration and data for the application.

Create New App Setup

✓ Select App

2 Configure App

3 Name and Description

4 Review and Apply

Configure App

Would you like to configure the application?

Yes

No

Configuration Details

🔍

Setting Category

Desktop orientation
Select the orientation of content displayed on an external monitor

Resolution and Size Mode
Select whether to automatically determine native resolution and screen size of external monitor (if possible) or to provide values manually.

Desktop orientation ⓘ

Discard Previous Next

Configuring the Do Not Change Setting

Setting a configuration to Do Not Change persists the previous configuration without making a change to the configuration. Enabling this setting does not alter the current setting. If you have never configured a setting, the default state persists.

An administrator may want to set a configuration to Do Not Change if the configuration is set to its default state or if the configuration is user-configurable and the administrator does not want to revert back to a default configuration upon a dock or undock event.

Setting Category

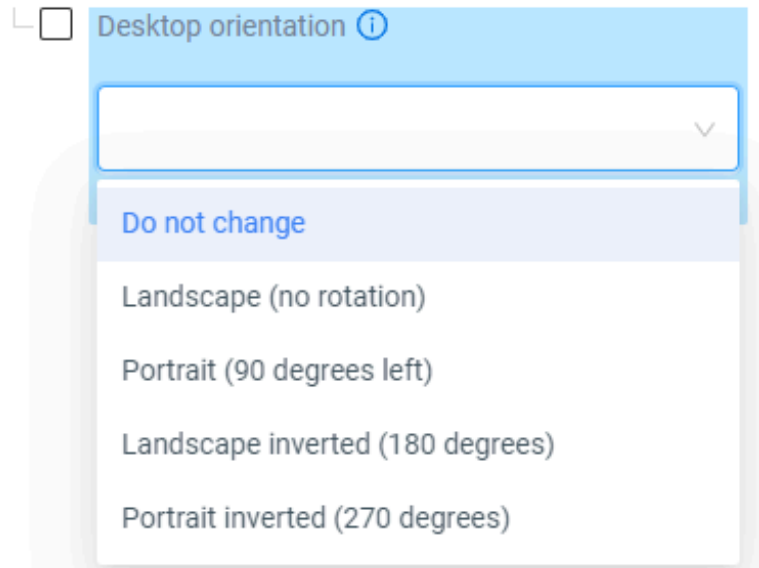
Desktop orientation

Select the orientation of content displayed on an external monitor

Resolution and Size Mode

Select whether to automatically determine native resolution and screen size of external monitor (if possible) or to provide values manually.

Desktop resolution



The screenshot shows a settings window titled "Desktop orientation" with an information icon. Below the title is a dropdown menu. The "Do not change" option is highlighted in blue. Other options listed are "Landscape (no rotation)", "Portrait (90 degrees left)", "Landscape inverted (180 degrees)", and "Portrait inverted (270 degrees)".

Configuring the External Monitor Orientation

Zebra Workstation Connect offers a method for the administrator to control the orientation of the external monitor. This setting should be configured to match the physical orientation that the display is intended to be used in to ensure that the content presented is properly oriented for viewing.

<p>Setting Category</p>	<p><input type="checkbox"/> Desktop orientation ⓘ</p>
<p>Desktop orientation Select the orientation of content displayed on an external monitor</p>	<p><input type="text"/></p>
<p>Resolution and Size Mode Select whether to automatically determine native resolution and screen size of external monitor (if possible) or to provide values manually.</p>	<p>Do not change</p>
<p>Desktop resolution Select the resolution of content displayed on an external monitor</p>	<p>Landscape (no rotation)</p> <p>Portrait (90 degrees left)</p> <p>Landscape inverted (180 degrees)</p> <p>Portrait inverted (270 degrees)</p>



NOTE: Rotation is not supported on ET5X devices.

Configuring Display Settings

Select **Automatic** as the **Resolution and Size Mode** to automatically choose the preferred Display Resolution and Display Density (content size) based on the specifications of the connected external display monitor and apply it, providing an adaptive viewing experience for the user.



NOTE: After connecting a new monitor, undock and re-dock the device to enable the new monitor connection or configuration.

<p>Setting Category</p>	<p><input checked="" type="checkbox"/> Resolution and Size Mode ⓘ</p>
<p>Desktop orientation Select the orientation of content displayed on an external monitor</p>	<p><input type="text"/></p>
<p>Resolution and Size Mode Select whether to automatically determine native resolution and screen size of external monitor (if possible) or to provide values manually.</p>	<p>Do not change</p> <p>Manual</p> <p>Automatic</p>



NOTE: It is recommended to set a resolution and density for managed configurations. Users can undock and re-dock the device to revert the resolution and density settings back to the default set by the admin if desirable.

If the administrator chooses to configure Display Settings, then the administrator-configured Display Settings are reapplied and override the user-configured Display Settings each time the device is docked. In such cases, the user can change them again, but the configuration is only in effect until the device is undocked. An administrator typically does this to ensure that all users of a shared device have a common experience on docking and are not negatively impacted by settings configured by a prior user of that shared device.

The default display settings are in place if the administrator does not decide to configure Display Settings. In this case, the user can change the Display Settings that remain set across multiple docks and undocks of the device. An administrator typically does this when a device is dedicated to a single user that does not share the device with other users with different roles.



NOTE: When the persist flag is set, all configurations previously applied to Zebra Workstation Connect are reapplied automatically when the application is reinstalled after an Enterprise Reset. When the persist flag is not set, all configurations previously applied to Zebra Workstation Connect are lost upon an Enterprise Reset and returns device settings to their defaults.

Configuring the External Monitor Resolution

Zebra Workstation Connect allows the administrator to control the resolution on a secondary screen (external monitor) by selecting a specific resolution from the menu.



NOTE: When these settings are applied using Zebra Workstation Connect managed configurations, they change the configuration of the underlying device. Therefore, the changes could continue to impact the UI after they are set if the device switches to Mirror Mode. Depending on the version of Workstation Connect you are using, you can switch between Desktop and Mirror Mode without rebooting the device.

Setting Category

Resolution and Size Mode

Select whether to automatically determine native resolution and screen size of external monitor (if possible) or to provide values manually.

Desktop resolution

Select the resolution of content displayed on an external monitor

Monitor size (deprecated)

Select the physical size of the external monitor. Zebra recommends entering the Screen Size (in inches) for best results.

Screen size (inches)

Enter the diagonal screen size (in inches) of the external monitor to be used. Resolution and monitor size are used to optimize the pixel density setting for the best user experience.

Desktop resolution ⓘ

Do not change

1920x1080

1920x1200

800x600

1024x600

1024x768

1280x720

Configuring External Monitor Density

Zebra Workstation Connect supports multiple methods to configure external monitor density. Providing Monitor Size (deprecated), Screen Size (recommended), or using Auto-detection allows Zebra Workstation Connect to render the application based on the specifications of the external desktop monitor.

Monitor Size

Selecting the Monitor Size is deprecated. While the feature is available for use, it is not the recommended way to calibrate external display settings. Configuring external display settings using Screen Size (inches) is recommended.



NOTE: Changing settings, such as the resolution density while in Always Docked mode, can disrupt the user's workflow if an application window is incorrectly calibrated.

<p>Setting Category</p> <hr/> <p>Desktop resolution Select the resolution of content displayed on an external monitor</p> <hr/> <p>Monitor size (deprecated) Select the physical size of the external monitor. Zebra recommends entering the Screen Size (in inches) for best results.</p> <hr/> <p>Screen size (inches) Enter the diagonal screen size (in inches) of the external monitor to be used. Resolution and monitor size are used to optimize the pixel density setting for the best user experience.</p>	<p><input checked="" type="checkbox"/> Monitor size (deprecated) ⓘ</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p style="text-align: right;">v</p> <p>Do not change</p> <p>Large</p> <p style="background-color: #e0e0e0;">Default</p> <p>Small</p> <p>Smaller</p> <p>Smallest</p> </div>
--	---

Screen Size (Inches)

Administrators can select the screen size in inches to inform the application to optimize its pixel density from the menu. Setting this value helps the application understand the native resolution of the external monitor and calibrate its output for the screen being used.

<p>Setting Category</p> <hr/> <p>Desktop resolution Select the resolution of content displayed on an external monitor</p> <hr/> <p>Monitor size (deprecated) Select the physical size of the external monitor. Zebra recommends entering the Screen Size (in inches) for best results.</p> <hr/> <p style="background-color: #e0e0e0;">Screen size (inches) Enter the diagonal screen size (in inches) of the external monitor to be used. Resolution and monitor size are used to optimize the pixel density setting for the best user experience.</p>	<p><input checked="" type="checkbox"/> Screen size (inches) ⓘ</p> <div style="border: 1px solid #ccc; height: 30px; margin-top: 5px;"></div>
---	---

Desktop UI Elements

Administrators can configure to show or hide UI elements on the desktop, including shortcuts, desktop wallpaper, contextual menu, notification panel, and taskbar. Users view a single application when all UI elements are set to Hide.

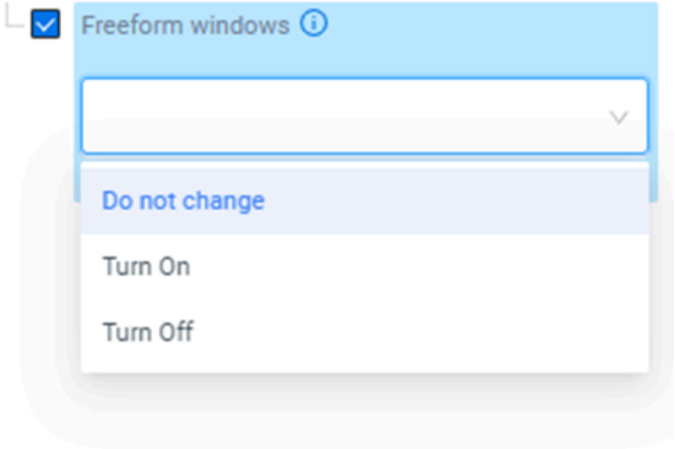
Enable the export managed configurations to allow users to export a set of configurations from the desktop home screen.

Setting Category	<input checked="" type="checkbox"/> Shortcuts ⓘ <input type="checkbox"/> Wallpaper ⓘ <input type="checkbox"/> Launcher Context Menu ⓘ <input type="checkbox"/> Notification Panel ⓘ <input type="checkbox"/> Taskbar ⓘ <input type="checkbox"/> Export managed configurations ⓘ
<p>Enter the diagonal screen size (in inches) of the external monitor to be used. Resolution and monitor size are used to optimize the pixel density setting for the best user experience.</p>	
Desktop UI Elements Open to configure Desktop UI Elements on the secondary screen	
Freeform windows Select whether apps on the secondary screen run within a movable, resizable window	
Status icons Open to configure the display of status icons on the desktop taskbar	
Desktop shortcuts Open to configure shortcuts on the desktop	
Wallpaper Open to configure wallpaper image and control manual configuration	
Application behaviors Open to configure various non-default application behaviors	
Screen Capture	

Configuring Freeform Windows

Administrators can enable or disable freeform windows to determine whether the application displays in a movable and resizable window. The application has a window control bar containing back, minimize,

and maximize/restore buttons when enabled. When disabled, the application launches with the window maximized and does not provide a control bar.

Setting Category	
<p>Enter the diagonal screen size (in inches) of the external monitor to be used. Resolution and monitor size are used to optimize the pixel density setting for the best user experience.</p>	
Desktop UI Elements Open to configure Desktop UI Elements on the secondary screen	
Freeform windows Select whether apps on the secondary screen run within a movable, resizable window	

Configuring the Visibility of Status Icons

The administrator can configure to show or hide icons presented to the user on the taskbar's status area. By default, the following status icons are displayed on the taskbar: Battery, Bluetooth, Cellular, Ethernet, VPN, Wi-Fi, Soft Input Panel (SIP), application settings, and audio settings. The administrator can choose to launch the corresponding device settings fragment when clicking on a specific status icon and launch the audio settings when clicking See More on the audio panel.

Setting Category	
Status icons Open to configure the display of status icons on the desktop taskbar	<input type="text"/>
Desktop shortcuts Open to configure shortcuts on the desktop	<input type="checkbox"/> VPN ⓘ <input type="text"/>
Wallpaper Open to configure wallpaper image and control manual configuration	<input type="checkbox"/> Wi-Fi ⓘ <input type="text"/>
Application behaviors Open to configure various non-default application behaviors	<input type="checkbox"/> SIP ⓘ <input type="text"/>
Screen Capture Select whether the device user is permitted to capture a desktop screenshot	<input type="checkbox"/> Settings UI from icons ⓘ <input type="text"/>
Desktop SIP Open to configure soft input panel for Desktop mode	<input type="checkbox"/> Audio settings from panel ⓘ <input type="text"/>
Taskbar Open to configure Taskbar options	
Device behaviors Open to configure various non-default mobile-device behaviors	

Sorting Desktop Shortcuts

Sort the shortcuts on the desktop home screen alphabetically or by the time or date added by selecting the preferred arrangement from the dropdown menu.

Importing Shortcuts

To import a file of shortcuts to deploy to a device ecosystem, enter the device path and filename of a shortcut file previously exported from a Zebra Workstation Connect application into the Shortcut import file field. When a shortcut import file is specified, this replaces all the current set of shortcuts. Administrators can also paste the contents of a shortcut file from a previously exported configuration. This form field accepts the path and file name of the same file in the device file system. When configuring the managed configuration, the full path should be provided: /enterprise/usr/zwc/filename.txt



NOTE: When using Workstation Connect version 1.5 or earlier, it is recommended to use the import shortcuts file path, then update Workstation Connect and export the shortcuts file again on the updated version of Workstation Connect that appends the checksum before mass deployment of the shortcuts file.

The administrator must deploy the file extracted from one device to the other devices that are going to be configured with that file in the device path. The filename entered into the form field must include the location in the device(s) where they are sending the managed configuration, and the file must be present in that place when the managed configuration is processed.



NOTE: When importing a file to create shortcuts, both /enterprise/usr and /data/tmp/public and subfolders are accepted. Shortcut export files are saved in /enterprise/usr.



NOTE: On EMM systems that limit the text size of input fields, some configurations might fail or be set incorrectly if the text pasted into the fields exceeds the limit set by the EMM. Ensure that the exported file size is within your EMM content limitation before mass deployment. Open the configuration file using a text editor in Windows to determine the size before pasting the contents into the EMM field.



NOTE: The recommended method of importing shortcuts is by pasting the file's contents into the Shortcut import file form field. While pasting contents of the file path is available, this feature is deprecated and may not be supported in future versions of Zebra Workstation Connect.

Mass Deploying Shortcuts

To replace all currently defined shortcuts with a set of application shortcuts defined by the administrator, select the Desktop Shortcuts option from the menu, as displayed in the following figure.

The screenshot shows the configuration interface for Desktop Shortcuts. On the left, a sidebar lists setting categories: Desktop shortcuts (selected), Wallpaper, Application behaviors, and Screen Capture. The main area displays the 'Add app' form with the following fields and controls:

- Add app** button
- Add app** (with an info icon)
- Package name** (with an info icon) and an empty text input field.
- Activity name** (with an info icon) and an empty text input field.
- Shortcut import file** (with an info icon) and an empty text input field.
- clear** and **delete** buttons.

A callout box points to the 'Shortcut import file' field with the text: "Paste the contents of a shortcuts file previously exported from ZWC desktop. Also accepts path and file name (deprecated) of the same file in the device file system."

Next, enter the package name and an activity name for each shortcut. The shortcut defaults to the application's main activity if the activity name is left blank. An administrator can specify an array of shortcuts within a set of managed configurations sent to Workstation Connect.

If no array is specified, no change is made by the application to the shortcuts shown on the desktop. This option is preferable if the administrator does not want to change the desktop shortcuts or the user can define them.

If an array is specified, it indicates the exact set of shortcuts that should be on the desktop and replaces any shortcuts on the desktop when applied to the device. Suppose the administrator has previously declared an array and intends to change the shortcut. In that case, the array must be re-defined to include all elements designed to be included in the new array. The application creates shortcuts on the desktop to match the specifications of the array.

Configuring the Desktop Home Screen Wallpaper

The administrator can change the default desktop home screen wallpaper to supported image files stored on the device and written to a location that is generally writable and readable by all applications, including images downloaded to the device by the administrator. This can be configured by using the image file's device path and file name to set as the desktop home screen wallpaper.

The file must be deployed to the device at the path and name specified before the managed configuration is applied. If this does not occur, the file is not processed. Changing the file after it has been processed does not cause the file to be reprocessed until the next time the managed configuration is applied.



NOTE: The maximum background resolution is 4000 x 2500. For optimal performance, use an image with a resolution that matches the resolution of the display being used.

<p>Setting Category</p>	<p><input type="checkbox"/> Wallpaper ⓘ</p>
<p>Desktop shortcuts Open to configure shortcuts on the desktop</p>	<p><input type="text"/></p>
<p>Wallpaper Open to configure wallpaper image and control manual configuration</p>	<p><input type="checkbox"/> User control ⓘ</p> <p><input type="text"/></p>
<p>Application behaviors Open to configure various non-default application behaviors</p>	

Using Immersive Mode

Workstation Connect supports configuration by the administrator to enable or disable automatic hiding of the taskbar for specific applications when running on the desktop in Immersive Mode. Automatic hiding of the taskbar upon entry or exit from Immersive Mode is disabled for all applications by default. Suppose the Alt+F4 keyboard shortcut is set to its default behavior. In that case, the shortcut closes the focused application even if the application is in Immersive Mode and then displays the previously hidden taskbar.

Not every application utilizes Immersive Mode in the same manner. The administrator can configure which application packages can hide the taskbar when the application is in Immersive Mode. The administrator must decide which applications use Immersive Mode and how the application handles entering or exiting from Immersive Mode.

The screenshot shows the configuration page for 'Application behaviors'. On the left is a sidebar with 'Setting Category' options: Desktop shortcuts, Wallpaper, Application behaviors (highlighted), Screen Capture, and Desktop SIP. The main area is titled 'Application behaviors' and contains several settings:

- Package name (with an info icon and a text input field)
- Activity name (with an info icon and a text input field)
- On Docking (with an info icon)
- On Undocking (with an info icon)
- Device-user Access (with an info icon)
- Immersive-mode Taskbar (with an info icon and a dropdown menu)

At the top right of the main area are 'clear' and 'delete' buttons. At the bottom, there is a section for 'Add App-related Files (Optional)' with columns for 'Google Drive', 'Linked File Detail', and 'File Path and Name on Target'.



NOTE: Firmware support does not identify applications beyond the package name.

Configuring Application Behaviors

To create a new application behavior, click **Add Application** behaviors.

- Specify the application package name and activity name. This field defaults to all application activities if the activity name is blank.

The screenshot shows the configuration interface for Application Behaviors. On the left is a 'Setting Category' sidebar with options: Application behaviors (selected), Screen Capture, Desktop SIP, and Taskbar. The main area shows a configuration form for 'Application behaviors'. At the top, there is a toggle for 'Application' and an 'Add Application behaviors' button. Below that, there is a toggle for 'Application behaviors' and 'clear' and 'delete' buttons. The form includes two input fields: 'Package name' and 'Activity name', each with an information icon.

- Next, specify the docking criteria that define the behavior that should be automatically performed for the application each time the device docks by selecting the **Action** and the **Window State** from the menu.
- The available actions are:
 - Stop** - indicates that the application should exit automatically if it is running on the mobile device when it docks. This is useful if the application has no relevance in desktop mode and uses resources that should be freed up upon docking to make them available for use by applications used in desktop mode.
 - Launch** - indicates that the application automatically launches on the desktop home screen at the time the mobile device docks. This would make the application available for use by the user without the need to launch it manually.
 - Move** - indicates that the application should be automatically moved from the mobile device to the desktop home screen if it is running on the mobile device when it docks. This is useful if the application is relevant and commonly used in mobile and desktop modes and in use cases where ongoing application use in desktop mode is feasible without needing to move it manually.



NOTE: Suppose the administrator does not specify the docking criteria. In that case, the default docking behavior for all applications keeps the application running on the mobile device (either foreground or minimized) and presents the corresponding icons on the taskbar.

Configure how the application is displayed when launched or moved on the desktop home screen by selecting its **Window State**. This setting only applies to Launch and Move actions and allows the administrator to determine whether the application is automatically maximized (shown full size) or restored (in default or last used size).

Setting Category	
Application behaviors Open to configure various non-default application behaviors	<input type="checkbox"/> On Docking ⓘ <input type="checkbox"/> Action ⓘ <input type="checkbox"/> Window state ⓘ <input type="checkbox"/> On Undocking ⓘ <input type="checkbox"/> Device Undocking ⓘ <input type="checkbox"/> Immersive-mode Taskbar ⓘ
Screen Capture Select whether the device user is permitted to capture a desktop screenshot	
Desktop SIP Open to configure soft input panel for Desktop mode	
Taskbar Open to configure Taskbar options	
Device behaviors	



NOTE: When setting the configuration to move an application upon a docking event, only one application should be configured to move when maximized.

- Set the undocking criteria that define the behavior that should be automatically performed for the application each time the device undocks by specifying the Action. The available actions for undocking criteria are stop, launch, and move.
 - Stop - indicates that the application should exit automatically if it runs on the desktop home screen when the device undocks. This is useful if the application has no relevance in mobile mode and demands resources that should be freed upon undocking to make them available for applications in mobile mode.
 - Launch - indicates that the application should automatically launch on the mobile device at the time the device undocks. This makes the application available for use by the user without the need to launch it manually.
 - Move - indicates that the application should automatically move from the desktop home screen to the mobile device if it runs on the desktop when it undocks. This might be appropriate if the application is used in mobile and desktop modes where ongoing application use in mobile mode is desirable without needing the user to move it manually.



NOTE: When undocking, if you are moving an application and prefer which one appears in the foreground, only specify the rule for that specific application intended to be viewed in the foreground. Only one application should be configured to open in the foreground after.



NOTE: Only one application can run in the foreground on the mobile device. Therefore, providing multiple launches/move undocking behaviors is not feasible. If done, the last application launched/moved becomes the foreground application, and the rest are minimized and accessed from the **Recents** panel.

Configuring Device User Access

This feature allows the administrator to control whether the user can launch specific applications from the Workstation Connect desktop home screen UI. Once the administrator configuration is applied, the Workstation Connect desktop UI is restricted to prevent the user from accessing the disabled method(s) to launch the restricted applications or settings on the external monitor.

Restrictions include the ability to individually or collectively prevent the following methods from being used to launch restricted applications or settings.

Administrators can allow or disable specific configurable options by selecting from the menu. Configurable options include:

- Enabling or blocking a user from launching a specified application from the Desktop All Apps Panel.
- Enabling or blocking a user from launching an application and its specified activities from an existing desktop shortcut.
- Enabling or blocking a user from launching all activities for the application from a notification in the notification panel.
- Enabling or blocking a user from moving all or specified activity for an application from the mobile computer to the desktop using the taskbar.

- Enabling or blocking a user from moving all or specified activity for an application from the desktop to the mobile computer from the taskbar.
- Enabling or blocking the visibility of specific application icons from displaying in the taskbar.



NOTE: If the intended use case does not require the device user to launch an application on the desktop, set all the parameters mentioned above to Disallow.

Configuring Screen Capture Permissions

Administrators have the capability to permit or restrict a user's ability to generate a screen capture of the secondary display by selecting Allow or Disallow from the associated menu. For some use cases, administrators might want to Disallow screen capture to protect sensitive data being displayed in an application on the desktop by preventing screen captures that could allow that data to be extracted from the device and shared without permission.

<p>Setting Category</p>	<p><input type="checkbox"/> Screen Capture ⓘ</p>
<p>Application behaviors</p> <p>Open to configure various non-default application behaviors</p>	<p>[Dropdown menu]</p>
<p>Screen Capture</p> <p>Select whether the device user is permitted to capture a desktop screenshot</p>	

Configuring the Desktop Soft Input Panel (SIP)

The SIP in desktop mode is configurable by entering the package and class name. The preferred SIP class name displays when the device is docked.



NOTE: Only one SIP can be set as the default.

Because there is only one default SIP configuration, Zebra Workstation Connect achieves the desired result by saving the default SIP on docking and changing the default SIP to the administrator-selected value. On undocking, Zebra Workstation Connect restores the saved default SIP. This allows a SIP optimized for desktop use while docked and one for mobile use when undocked.

Setting Category	<input type="checkbox"/> Package name ⓘ <input type="text"/>
Desktop SIP Open to configure soft input panel for Desktop mode	<input type="checkbox"/> Class name ⓘ <input type="text"/>
Taskbar Open to configure Taskbar options	
Device behaviors Open to configure various non-default mobile-device behaviors	

Enabling or Disabling the All Applications Button

This setting allows the administrator to prevent users from accessing applications on the desktop home screen from the All Applications button on the taskbar. When the All Applications button is disabled, the user can access or launch applications from the shortcuts displayed on the desktop, notification panel, status icons, and home screen unless prohibited by the administrator.

Setting Category	<input type="checkbox"/> All Apps Button ⓘ <input type="text"/>
Desktop SIP Open to configure soft input panel for Desktop mode	<input type="checkbox"/> Mobile App Icons ⓘ <input type="text"/>
Taskbar Open to configure Taskbar options	
Device behaviors Open to configure various non-default mobile-device behaviors	

Configuring Device Behavior

Administrators can configure whether the mobile device screen is dimmed upon docking by turning this option on or off from the menu. This setting is helpful for use cases where work is being done exclusively on the external monitor, and the administrator does not want to distract the user with content that could display on the device screen or the administrator seeks to protect potentially sensitive data from being displayed on the device screen. Wake the device from the dim setting by pressing the power button.

Setting Category

Desktop SIP

Open to configure soft input panel for Desktop mode

Taskbar

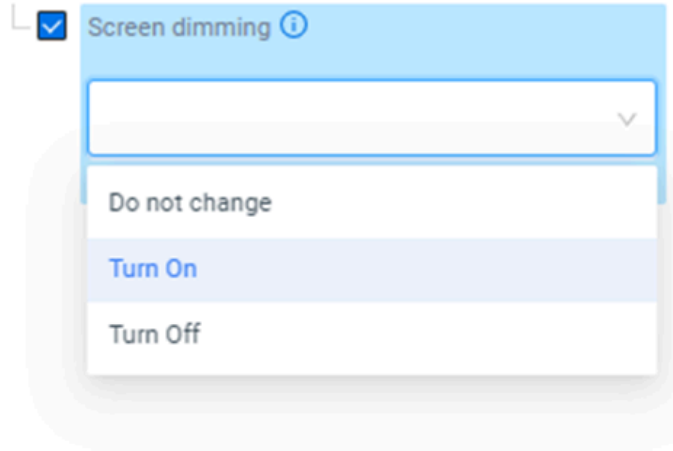
Open to configure Taskbar options

Device behaviors

Open to configure various non-default mobile-device behaviors

Persistence

Select whether ZWC configurations should remain on the device following an Enterprise Reset



Enabling Persistence

Determine whether Zebra Workstation Connect configurations should remain on the device following an Enterprise Reset by selecting Turn On or Turn Off from the menu.



NOTE: When persisting managed configurations across an Enterprise Reboot, using the Zebra Workstation Connect configuration reset field is recommended. Do not persist the file using FileMgr.

Setting Category

Desktop SIP

Open to configure soft input panel for Desktop mode

Taskbar

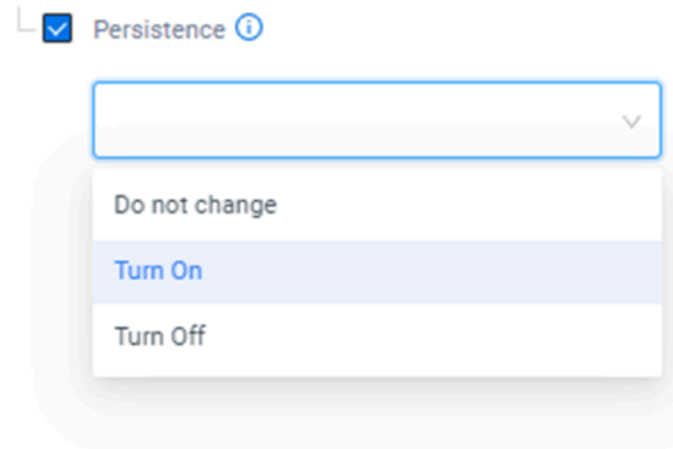
Open to configure Taskbar options

Device behaviors

Open to configure various non-default mobile-device behaviors

Persistence

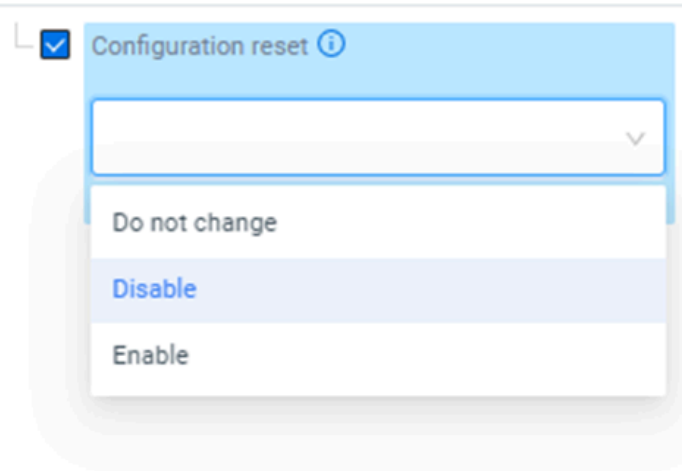
Select whether ZWC configurations should remain on the device following an Enterprise Reset



Resetting the Current Configuration

Enable or disable the device user's ability to reset the Zebra Workstation Connect configuration to its default state.

Setting Category
Desktop SIP Open to configure soft input panel for Desktop mode
Taskbar Open to configure Taskbar options
Device behaviors Open to configure various non-default mobile-device behaviors
Persistence Select whether ZWC configurations should remain on the device following an Enterprise Reset
Configuration reset Select whether to allow the device user to reset all ZWC settings to their default state



Update Behavior

Configure when the device user experiences the behavior defined by the configuration changes.

On the next dock, wait until the device is undocked and re-docked into the cradle before the configuration changes are observed.

Selecting immediately implements the configuration changes to Zebra Workstation Connect instantly. As a result, use caution when this option is enabled, as the configuration changes could interrupt a user's workflow.

Setting Category

Desktop SIP

Open to configure soft input panel for Desktop mode

Taskbar

Open to configure Taskbar options

Device behaviors

Open to configure various non-default mobile-device behaviors

Persistence

Select whether ZWC configurations should remain on the device following an Enterprise Reset

Configuration reset

Select whether to allow the device user to reset all ZWC settings to their default state

Update behavior

Select when the behavior defined by configuration changes are experienced by the device user

Update behavior ⓘ

[Dropdown menu]

Do not change

On Next Dock

Immediately



NOTE: New configuration behaviors cannot be implemented immediately on L10 devices.

Versioning

Enter a version number to identify the configuration being pushed to the device ecosystem. This is useful for the administrator to manage different configurations by providing an identifier.

Setting Category	<input checked="" type="checkbox"/> Version ⓘ
Desktop SIP Open to configure soft input panel for Desktop mode	<input type="text"/>
Taskbar Open to configure Taskbar options	
Device behaviors Open to configure various non-default mobile-device behaviors	
Persistence Select whether ZWC configurations should remain on the device following an Enterprise Reset	
Configuration reset Select whether to allow the device user to reset all ZWC settings to their default state	
Update behavior Select when the behavior defined by configuration changes are experienced by the device user	
Version Enter a version to identify the config being pushed	

Using the Feedback Channel

Use the Google Feedback Channel to send results in keyed application states to the EMM from pushed managed configurations to the device. Once a managed configuration is received, Workstation Connect processes the configuration to validate the data and sends feedback to the EMM indicating if Workstation Connect accepted or rejected the data. After validating the configuration data, Workstation Connect sends a **SEVERITY_INFO** or **SEVERITY_ERROR** as a feedback message with further information.

- **SEVERITY_INFO** indicates that the configuration is correct, and the confirmation message displays the changes made by applying the new configuration.

- **SEVERITY_ERROR** indicates that the configuration is incorrect and no change has occurred. Observe the feedback message to understand why. Make the appropriate changes and reapply the configuration.

Using Generic Intents

Zebra Workstation Connect allows administrators to define intents that can be used to employ different actions supported by Android for intra-and inter-application communication on the device. Create a shortcut for a specifically defined intent to quickly access different actions such as playing media or taking a screenshot.



NOTE: When using Generic Intents, the administrator is responsible for testing the intent before setting the intent using Workstation Connect. Intents are processed differently depending on the application or Android Version.

Editing the Name and Description of the Configuration

When the configuration of Zebra Workstation Connect is completed, follow the steps below to apply the configurations to the corresponding devices:

1. Enter a **Name** and **Description** for the profile, or use the auto-generated name. Click **Next** to proceed.

Create New App Setup

X

✓ Select App

✓ Configure App

3 Name and Description

4 Review and Apply

App Setup Name

✖

You can edit the automatically generated name.

App Setup Description

You can write down your notes, such as what this setup is for, what kind of the setup is, etc.

Please enter app setup description

Discard
Previous
Next

- Review the settings. Click **Apply Now** to deploy the settings immediately or click **Save** to save the configuration for later deployment.

Create New App Setup X

- Select App
- Configure App
- Name and Description
- Review and Apply**

App Setup Name Edit

app_setup_20231025_221251

App Setup Description Edit

App Details Edit

APP NAME	HOSTING LOCATION	APP VERSION	DEVELOPER	PACKAGE NAME	APP DESCRIPTION
Zebra Workstation Co...	Specified Server	2.0.7		com.zebra.workstatio...	

Configure App Edit

Yes

Save
Previous **Apply Now**

- Select the device to configure and click **Apply**..

System Configuration Features

The following sections describe tools that enable the administrator to apply system configurations on the mobile device, including the ability to disable USB storage, configure user access to settings, install or uninstall applications, launch, enable or configure applications, configure keyboard layout, and configure USB scanners and screen sharing.

Administrators can implement system configurations through Staging (using StageNow) or an EMM. Depending on the EMM, configurations are implemented directly through the EMM, OEMConfig, or MX (if supported).

Preventing Automatic Application Updates

When using an EMM to deploy Zebra Workstation Connect from the Playstore, the APK is automatically updated to the latest version. The Operating System is not automatically updated, causing the potential for a version mismatch between the Operating System and APK.

If an administrator decides to defer updating to a new BSP and a new version of Zebra Workstation Connect is posted to the Playstore. This allows the Playstore or an EMM to update Workstation Connect to the latest version automatically. This is not recommended because it can cause a version mismatch.

To protect against a version mismatch, use AppMgr settings to prevent the APK from automatically updating by blocking specific applications from automatically updating by package name. When this function is enabled, only the tool can update applications. To allow applications to update automatically, disable the tool.

For additional information, go to techdocs.zebra.com/mx/appmgr/.

Keyboard Configuration

Workstation Connect supports configuration by the administrator of one or more keyboard name/layout name mappings when there is no physical keyboard connected to the cradle. The application automatically detects when a keyboard is connected and uses the mapped or default layout based on whether a mapping exists for the detected keyboard. This feature is helpful for use cases with multiple keyboard language layouts.

The following functions support managing keyboard mappings:

1. Add/Replace - Add a new mapping for a named keyboard or replace any existing mapping for a named keyboard (will cause any keyboard with a matching name to subsequently use that layout)
2. Remove - Remove an existing mapping for a named keyboard (will cause any keyboard with a matching name to subsequently use the default layout)
3. Remove All - Remove all existing mappings for all keyboards (causes all keyboards to use default layouts subsequently).

For additional information on configuring this option using OEMConfig, go to techdocs.zebra.com/oemconfig/11-2/mc/#steps.step.uiStep.uiExternalKeyboardConfig

For additional information on compatible keyboard mappings and shortcut configuration, go to techdocs.zebra.com/mx/uimgr/#external-keyboard-action

External Keyboard Num-Lock

Configure Num-lock on an external keyboard using UI Manager for use cases where users mostly use the numbers on the keyboard instead of arrow keys.

External Keyboard Shortcut Action and ID

Zebra Workstation Connect leverages UI Manager to define how the device handles shortcut-key events from the external keyboard.

First, choose an action for handling shortcut key events (do not change, ignore, perform standard handling, or send to an application running in the foreground). Then, assign the action for the specified shortcut key to employ when the key is triggered.



NOTE: Some shortcut keys are enabled by default. Use UI manager to disable shortcut keys that you do not use and may interrupt your workflow.

Password Characters Show/Hide

UI Manager controls whether each password character is displayed briefly on the screen as it is entered; otherwise masked at all times. This parameter controls the Security & Location function of the Settings panel.

For additional information, go to: techdocs.zebra.com/mx/uimgr/.

USB Scanner Configuration

Workstation Connect supports using a USB scanner configured via an appropriate system configuration. Administrators can also configure specific barcode input options within a Datawedge profile for use when scanning.



NOTE: Barcode scanners connected to the cradle must be set up in SSI mode to function correctly with Workstation Connect.

Visit the product-specific Programmer's Reference Guide at zebra.com/support for information about switching modes.

For additional information, go to techdocs.zebra.com/datawedge/11-2/guide/input/barcode/#scannerselection

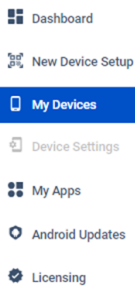
Remote Control and Screen Share

Administrators can choose which screen is used to view standard collaboration tools. This feature is helpful for use cases where the user seeks to share information on the external monitor with a colleague or customer.

Zebra DNA Cloud version 2.7 or higher provides the ability to remote control a user's mobile device or desktop home screen.

To enable this functionality using Zebra DNA Cloud:

1. Navigate to the **My Devices** screen and click **Remote Support**.



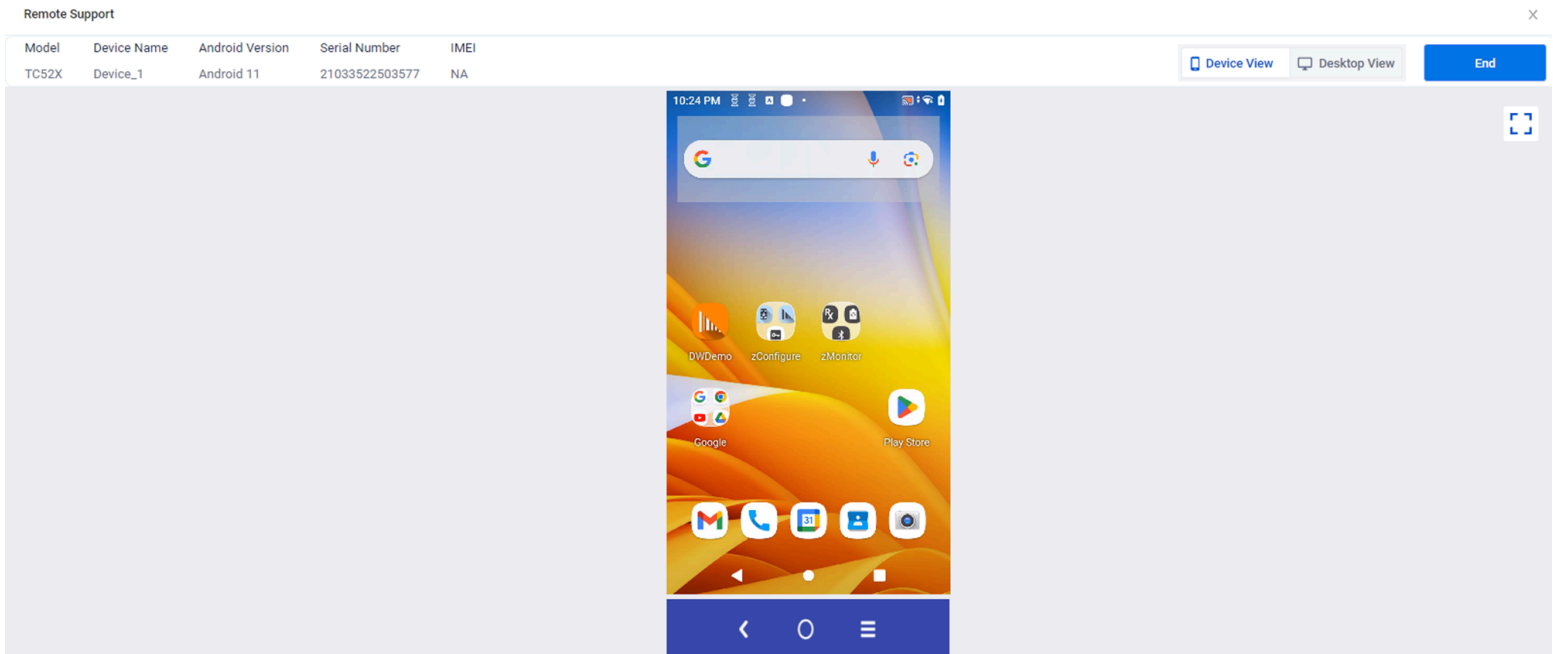
My Devices

Here you can view and manage all your devices.

<input type="checkbox"/>	MODEL	DEVICE NAME	DEVICE GROUP	OS VERSION	SECURITY PATCH DATE	SERIAL NUMBER	IMEI	BATTERY HEALTH	ACTIONS
<input type="checkbox"/>	TC52X	Device_1		Android 11	2023-01-05	21033522503577	NA	🟢	

1-1 of 1 Devices 1 25 Devices / Page

2. Observe the **Remote Support** window to view the device screen and device information to control the device remotely through the browser window.



Support for remote control is dependent upon the tool; consult the tool vendor to determine compatibility. If the tool supports remote control, ensure that you are using the latest version of the EventInjectorService. You must grant access using AccessMgr. For additional information on using AccessMgr, go to techdocs.zebra.com/stagenow/2-9/csp/access/. The process for each application is specific to the tool and its vendor. Consult the tool vendor to understand the process specific to the tool you intend to use.



NOTE: EventInjectionService version 4.8.2 or higher must use the dual-screen remote control on Zebra Workstation Connect.

Some Remote Control and collaboration tools may offer an integrated facility to select which screen to view/control or view/control both screens simultaneously. When a given tool does not support this, Zebra provides a means to do so from outside such tools.

For additional information, go to techdocs.zebra.com/oemconfig/11-2/mc/#steps.step.displayStep.

Administrators can connect to the device, view, and control that device's screen for use cases requiring remote assistance. This capability is helpful for use cases where a user must relinquish the application's control to allow a different user to complete a specific task.

For additional information, go to techdocs.zebra.com/mx/displaymgr/.



NOTE: Remote viewing and remote control with device screen rotation are not supported on ET5X devices.

Supporting Zebra Enterprise Applications

Enterprise Browser and Enterprise Keyboard enhance the user experience when utilized with Zebra Workstation Connect. These applications integrate seamlessly with Zebra Workstation Connect, whereas third-party applications may necessitate additional steps for full customization. For example, Enterprise

Browser is an industrial browser that provides the tools to rapidly build device applications for barcode scanning, signature capture, payment processing, and printing on all Zebra-supported devices.

For additional information on Enterprise Browser, go to techdocs.zebra.com/enterprise-browser/3-2/guide/about/

For additional information on Enterprise Keyboard, go to techdocs.zebra.com/mx/enterprisekeyboardmgr/

Configuring the Audio UI

Configure audio settings using the AudioVolUIMgr CSP. For additional information about using the AudioVolUIMgr, go to techdocs.zebra.com/stagenow/5-4/csp/audiomgr/. This method allows administrators to set a minimum and maximum volume setting that the user cannot go below or exceed.

For additional information on configuring this option using OEMConfig, go to: techdocs.zebra.com/oemconfig/11-2/mc/#steps.step.audioStep.

Best path routing determines the audio output of the application. For additional information on preferred path configurations, go to the Audio Manager CSP techdocs.zebra.com/stagenow/5-4/csp/audio/.

If the administrator does not configure a specified audio configuration, the default Android audio settings are enabled.

Review the pathway outlined below to understand how the application prioritizes audio outputs.

Best Available Audio Output Paths

Suppose there are specific audio paths that the administrator does not intend to use. In that case, configure the best audio path to ensure that specific paths are unavailable to the user. Selecting a specific audio path can reduce frustration for users that might have to override an incorrect choice over and over.

The user can change the audio path from the Desktop Audio Panel. However, the user's choice may be overridden upon a dock or undock event, depending upon the administrator's configuration.



NOTE: Preventing an audio path from being chosen as optimal does not restrict the user from overriding that path. Instead, it prevents the system from selecting it automatically.



NOTE: Each time the set of audio devices changes (including docking and undocking), the best path routing recalibrates and overrides any previous setting implemented by the user.

Android has a specific methodology for best path routing that is automatically applied if the administrator does not change the default configuration.

1. Cradle/Dock (USB is unavailable upon docking the device)
 - a) Headset
 - b) Headphones/speaker
2. Mobile Device Analog (3.5mm - treated as a USB headset)
 - a) Headset
 - b) Headphones
3. Bluetooth Connected Device
 - a) Headset
 - b) Headphones/speaker

4. Monitor (HDMI is unavailable upon docking)
 - a) Headphones/speaker (USB or 3.5mm)
 - b) Integrated Speaker
5. Mobile Device Headset (Unavailable upon docking)
 - a) Integrated Microphone
 - b) Integrated Speaker
6. Mobile Device Speakerphone

Optimizing User Access to Applications

Many EMMs provide ways for administrators to configure user access to application settings to fit a specific use case. The tables below outline common access points to applications, ways that EMMs enable or disable their visibility to users, and strategies to use Zebra Workstation Connect to leverage them based on common use cases for specific applications by administrator configuration settings.

Table 2 Administrator Configuration Settings

Configuration Number	Administrator Configuration Setting
1	Disable Application behaviors > Taskbar Move to Device
2	Disable Application behaviors > Taskbar Move to Desktop
3	Disable Application behaviors > Taskbar Icon
4	Disable Application behaviors > All Apps
5	Disable Application behaviors > Create Shortcut
6	Disable Application behaviors > Launch Shortcut
7	Disable Application behaviors > Notification
8	Disable Application behaviors > On Undocking > Stop

Table 3 Application Settings Strategy

Category	Description	Administrator Configuration Strategy
A	Applications intended to run on both primary and secondary screens.	Additional optional administrator configurations may support the use case.
B	Applications intended to run only on the secondary monitor	Administrator configuration 1 or 3
		Administrator Configuration #8
C	Applications intended to run on mobile only.	Block the application on the primary launcher based on the primary launcher settings.
		Administrator configuration #2 or #3
		Administrator configuration #4

Table 3 Application Settings Strategy (Continued)

Category	Description	Administrator Configuration Strategy
		Administrator configuration #5 Administrator configuration #6 Administrator configuration #7 Do not create a shortcut for the application by default. Do not create a rule to move the application to the secondary screen when docking.
D	Applications that do not run on primary or secondary screens.	Administrator configuration #3 Administrator configuration #4 Administrator configuration #5 Administrator configuration #6 Administrator configuration #7 Do not create a shortcut for the application by default. Block the application on the primary launcher based on the primary launcher settings. Do not create a rule to launch the application to the primary or secondary screen when docking or undocking.
E	Applications that are intended to always run in the background without any interaction with the end user	Administrator configuration #3 Administrator configuration #4 Administrator configuration #5 Administrator configuration #6 Administrator configuration #7 Do not create a shortcut for the application by default. Block the application on the primary launcher based on the primary launcher settings. Do not create a rule to launch the application to the primary or secondary screen when docking or undocking.
F	Primary launchers that utilize Lock Task Mode (for example, Airwatch Launcher)	Use the EMM to allow the ZWC and DisplayLink applications. Use the EMM to allow every application that is in application categories A, B, or C.

Table 3 Application Settings Strategy (Continued)

Category	Description	Administrator Configuration Strategy
		Administrator configuration #3
		Administrator configuration #4
		Administrator configuration #5
		Administrator configuration #6
		Administrator configuration #7
		Do not create a shortcut for the application by default.
		Do not create a rule to move the application to the secondary screen when docking.

Guidelines for Kiosk Behavior

In some cases, using Zebra Workstation Connect to implement kiosk-like application behavior is desirable. Consider a use case where the UI presented by Zebra Workstation Connect is exposed to the public, such as in a physical kiosk located within a retail establishment where customers interact with the UI to perform some targeted function(s). For example, the user might browse deals, print coupons, search for items in stock, review item prices, and so on.

In this case, limiting the options for customer interaction with the UI is desirable to prevent mistakes or malicious actions. For example, an administrator might want to lock the user into a task-specific application and prevent the user from exiting or launching any other applications.

Administrator Configuration	Guidelines for Use
Edit Desktop UI Elements > Hide Shortcuts	Select whether shortcuts display on the secondary screen
Edit Desktop UI Elements > Hide Wallpaper	Select whether a wallpaper displays on the secondary screen
Edit Desktop UI Elements > Hide Launcher Context Menu	Select whether to display a Context Menu when right-clicking on the desktop
Edit Desktop UI Elements > Hide Notification Panel	Select whether the Notification Panel displays on the secondary screen
Edit Desktop UI Elements > Hide Taskbar	Select whether a Taskbar displays on the secondary screen
Disable Freeform Windows	Select whether applications on the secondary screen run within a movable, resizable window.
Disable Application behaviors > Taskbar Move to Device	Select whether a device user can move all or specified activity for the application from the desktop to the device.

Administrator Configuration	Guidelines for Use
Disable Application behaviors > Taskbar Move to Desktop	Select whether a device user can move all or specified activity for the application from the device to the desktop.
Disable Application behaviors > Taskbar Icon	Select whether a taskbar icon is shown for the application when running.
Disable Application behaviors > All Apps	Select whether a device user can launch all or specified activity for the application from the desktop all apps panel.
Disable Application behaviors > Create a Shortcut	Select whether a device user can access all or specified activity for the application to be added as a shortcut
Disable Application behaviors > Launch Shortcut	Select whether a device user can launch all or specified activity for the application to be added as a shortcut
Disable Application behaviors > Notification	Select whether a device user can move all or activities for the application from a notification in the notification panel
Disable Application behaviors > On Undocking > Stop	Select whether a device user can move all or specified activity upon an undocking event
Taskbar > All Apps Button > Disable	Select whether clicking the All Apps button displays the All Apps panel.
Taskbar > Mobile App Icons > Hide	Select whether icons of running mobile applications are displayed



NOTE: Any time a physical keyboard is connected, keyboard shortcuts initiated from the keyboard will perform their normal functions. In many cases, this could provide the user with inappropriate functionality. In such cases, it may be ideal to avoid providing access to the keyboard to the user. For example, a touch monitor might be used instead of a keyboard to limit user access to functions offered on-screen by an application.



NOTE: The PrintScreen keyboard shortcut can capture a screenshot; however, no toast notification displays.



NOTE: When applications run with this specific behavior, users can still use the contextual menu by right-clicking the desktop shortcuts or the applications running on the Taskbar.

The following configurations could collectively achieve complete kiosk lockdown or in subsets to satisfy other less extreme use cases.

Zebra Workstation Connect has a collection of configurations that can strategically limit the visibility of specific UI elements in various ways. Together, these configurations define the UI sufficiently to implement a stand-alone kiosk safely. An administrator may choose to apply some or all available configurations. If users require additional access, relaxing the restrictions to suit their needs could be helpful.

To achieve kiosk behavior:

- Turn freeform windows off by forcing an application to run maximized without a window control bar. This would make more screen space available for displaying application content and ensure that the user could not close or minimize the application because the buttons are on the window control bar,

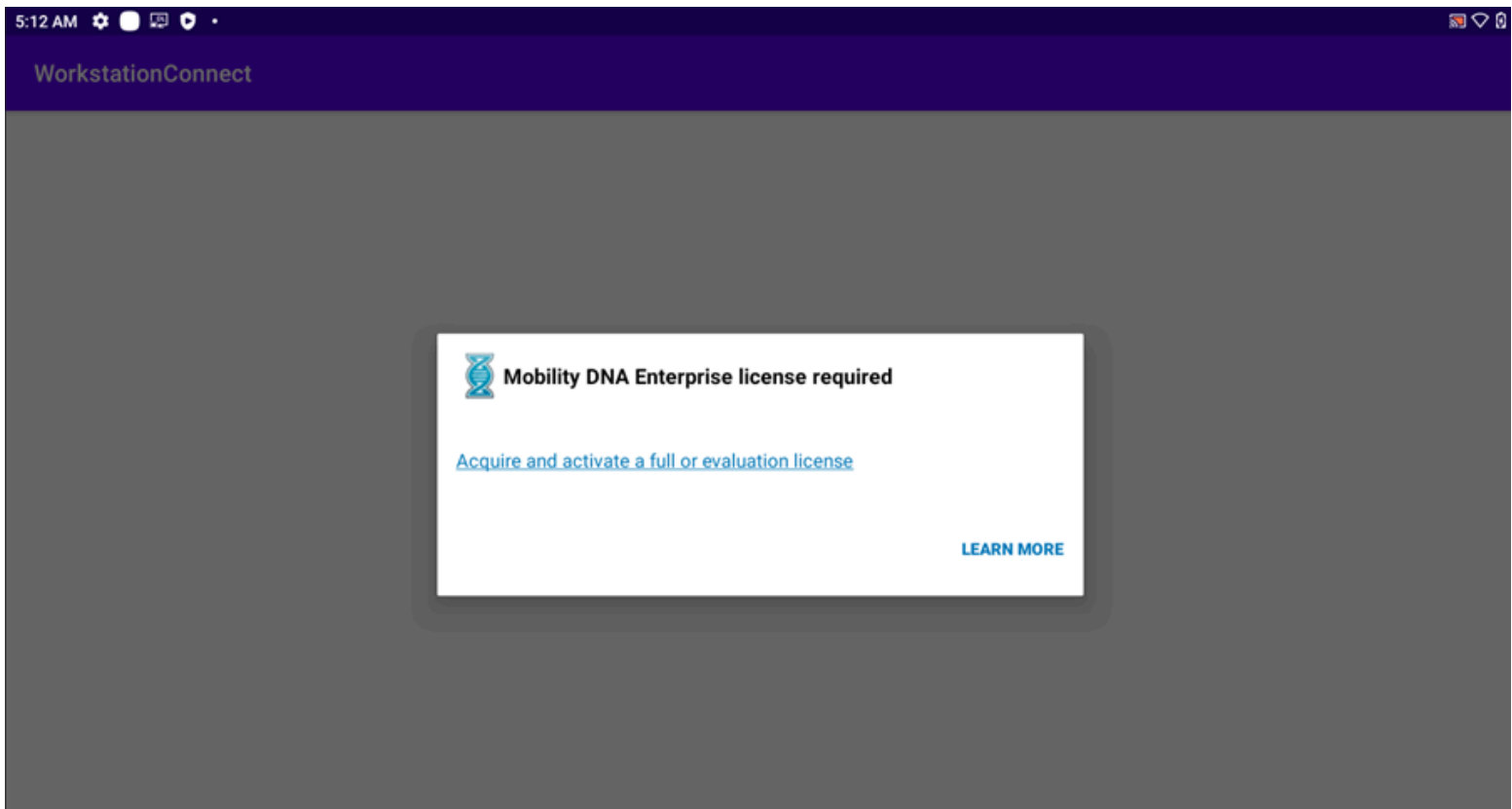
which is not shown. This would also ensure that the user could not resize the application, exposing the desktop or other applications. To exit such an application, the user would typically need to complete that application's task(s) to its satisfaction. At that point, the application could elect to exit, exposing the desktop or launch another application to take its place.

- Turn the Taskbar off by preventing the user from seeing what applications are running and from using the icons on the Taskbar to close, reset, or switch between those applications.
- Control which shortcuts are displayed on the desktop and disable the user's ability to create and modify shortcuts. This allows the user to launch applications approved for use but prevents the user from launching any applications not approved for use.

For use cases that do not require complete kiosk behavior, it may be optimal to block selected items from the Launcher Context Menu (such as Shortcut or Wallpaper) rather than block access to the entire Launcher Context Menu. Other items on the Launcher Context Menu (such as Suspend and Lock device) can be helpful for users to have access to in case slight adjustments are needed that do not necessitate intervention from the administrator.

MDNA Licensing

Zebra Workstation Connect is included premium-tier devices at no additional cost. To use Zebra Workstation Connect on value-tier devices such as ET4X or TC21/26, you must acquire an MDNA license and deploy it as part of the system configuration. This step is required to activate Zebra Workstation Connect, and the application does not run on the device if the license is not on the device.



For more information, go to techdocs.zebra.com/licensing/process/



NOTE: The device must reboot after the license is activated.

L10 Tablet Considerations

When using Workstation Connect with an L10 tablet, ensure that you are familiar with the device features and its constraints when docked in a cradle.

For additional information, go to the L10 tablet support page on zebra.com/support

Version Support

A device-initiated feature incompatible with the Zebra Workstation Connect version that you are using might still present the UI. If you attempt to use a feature that is present in the UI but not supported in the version of the application that you are using, a dialog box displays informing you that your version of Workstation Connect does not support the feature you are trying to use.

Secure Mass Deployment of Managed Configurations

Zebra Workstation Connect supports the secure mass deployment of managed configuration files using a JSON file delivered by Storage Secure Manager (SSM). Configuration files are deployed using StageNow or programmatically within your application.

The JSON configuration file name must be `workstation_connect_config.txt` and placed in the `/enterprise/usr` or `/data/tmp/public` paths only.

Use the process outlined in StageNow to push the configuration file to these two locations. If you are using an EMM, follow the process specified by the EMM.

Create a configuration barcode using FileMgr in StageNow to inform the SSM to deliver the JSON file from the folder to Zebra Workstation Connect. Next, use StageNow to scan the configuration barcode.



NOTE: Copying the managed configuration file from one folder to another is not supported.

For additional information on deploying managed configurations using StageNow or programmatically within your application, go to techdocs.zebra.com/ssm/1-1/guide/deploy/.



NOTE: When persisting managed configurations across an Enterprise Reboot, using the Zebra Workstation Connect configuration reset field is recommended. Do not persist the file using FileMgr.

Lock-task Mode

Lock-task mode blocks all applications from launching except those specified on the AllowList.



NOTE: Administrators must add Zebra Workstation Connect and DisplayLink to the list of allowed applications by providing their package name prior to enabling Lock-task mode. Zebra Workstation Connect and DisplayLink must be on the AllowList.

Administrators must ensure that the applications defined in the docking and undocking rules are added to the AllowList in Lock-task mode. It is not necessary to configure rules for applications that are not used in Lock-task mode.

When a device is in Lock-task mode, the following screen elements display for applications that are on the AllowList:

- The All Apps panel
- Desktop shortcuts
- Add shortcut menu
- Notifications panel (shows notifications of allowed applications only)
- Taskbar showing running applications

When applications on the AllowList are pushed to the Lock-task mode profile from an EMM, changes apply to the device immediately. However, a device undock and redock is required for the changes to apply to the desktop home screen on the external monitor. Applications with defined rules for docking and undocking must be added to the AllowList.

Application shortcuts that link to approved applications perform as expected. Shortcuts for web links, files and intents are displayed, but perform as expected only if the application required to launch the shortcut is added to the AllowList.



NOTE: If the device is rebooted while docked, the device must be undocked and redocked for changes to apply.

Troubleshooting

This section describes potential issues that could arise while using Zebra Workstation Connect and solutions that could correct the problem, such as undocking and docking the device or performing a reboot.

Table 4 Troubleshooting

Source	Problem	Cause	Solution
Device (Workstation Cradle with Mobile Computer or Tablet)	External monitor not detected.	The device is powered off when placed in the cradle and then turns on.	Remove the device from the cradle and re-insert it. The device will then detect the monitor.
	The display does not change orientation quickly.	It takes a little time for the device to recognize the monitor.	Wait for the screen to re-orientate.
		The device is not detecting the monitor.	Remove the device from the cradle and re-insert it.
	Peripheral not detected.	Display setting not set properly	Go to Settings > Display > When the device detects an external monitor. Ensure Rotate screen orientation is selected.
		Bad cable connection.	Remove the cable and re-connect.
	External monitor blank.	Screen capture is disabled by default when setting a new Device Owner.	Enable screen capture during enrollment.

