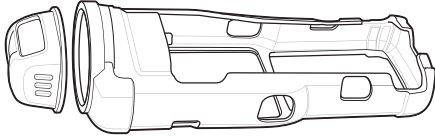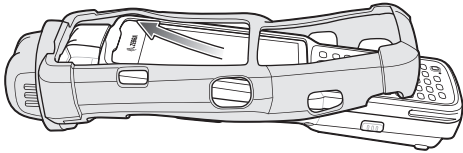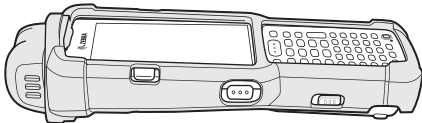Figure 125   Two Piece Rubber Boot

2. Slide the top of the MC3300x-R into the top of the rubber boot.

Figure 126   Attach Top of Rubber Boot

3. Grasp the bottom of the rubber boot and place over the bottom of the MC3300x-R.

Figure 127   Attach Bottom of Rubber Boot

NOTE: To function properly, remove the entire rubber boot from the device before placing the device in a charging cradle or rigid holster.
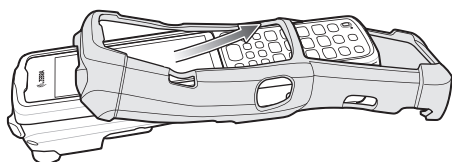
MC3300x-S Rubber Boot

The rubber boot provides additional protection to the MC3300x-S.
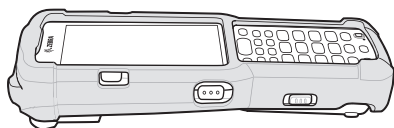
To attach the rubber boot:

1. Slide the bottom of the MC3300x-S into the bottom of the rubber boot.

Figure 128   Attach Bottom of Rubber Boot

2. Grasp the top of the rubber boot and place over the top of the MC3300x-S.

Figure 129   Attach Top of Rubber Boot

NOTE: To function properly, remove the entire rubber boot from the device before placing the device in a charging cradle or rigid holster.

Rigid Holster

The Rigid Holster provides a holder for the MC3300x-R/S. It consists of a mobile computer holder and a detachable belt clip. Press the release button to remove the detachable belt clip.

Figure 130   Plastic Holster

Detachable Belt

Release Button

Mobile Computer

Figure 131   Attaching the Rigid Holster

Clip Release

Mobile Computer Holder
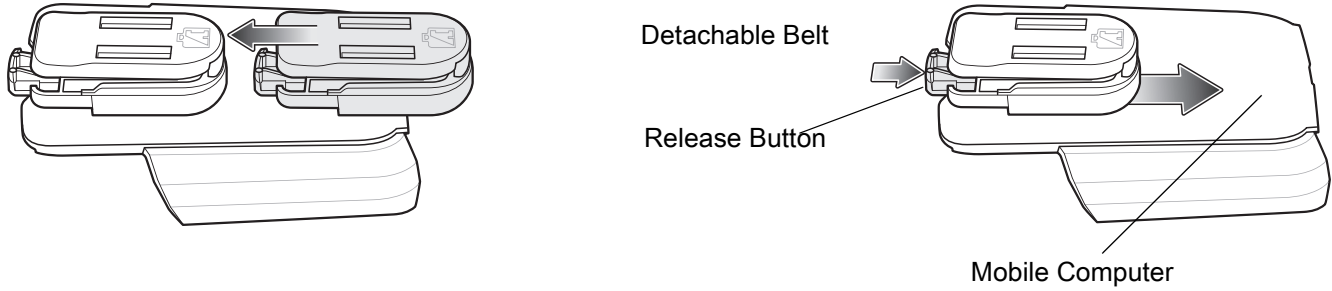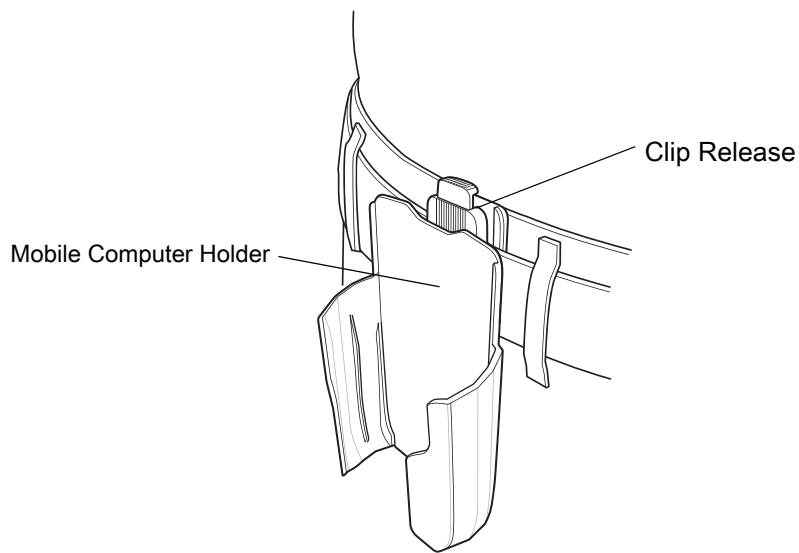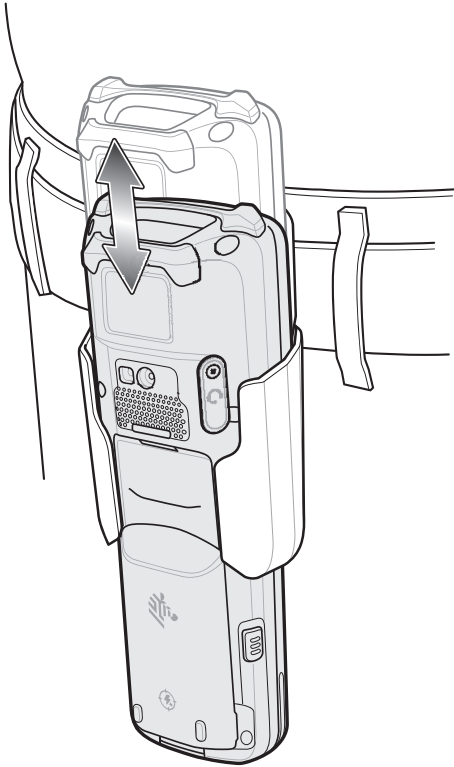
The Rigid Holster holds the mobile computer on a belt or waist band.

To insert the mobile computer, slide the mobile computer into the Rigid Holster with the screen facing the user.

To remove the mobile computer, press and lift to remove the mobile computer.

Figure 132   Insert and Remove the Mobile Computer

NOTE: To function properly, remove the entire rubber boot from the device before placing the device in a rigid holster.

MC3300x-G Fabric Holster

The fabric holster provides a soft holder for the mobile computer. It consists of a fabric mobile computer holder, a detachable shoulder strap and a belt strap. See figures below to attach the fabric holster to a belt and shoulder strap.

Belt Strap

Attach the fabric holster to a belt or waist band.

Figure 133   Attach the Fabric Holster to a Belt
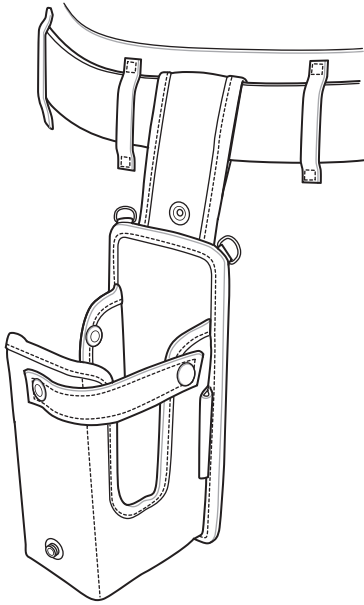
Shoulder Strap

Attach the fabric holster to a shoulder strap.

Figure 134   Attach the Fabric Holster to a Shoulder Strap
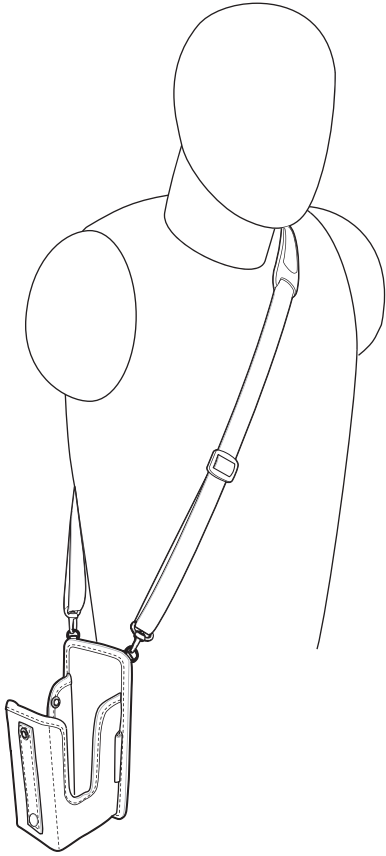
Using the Belt Strap

The fabric holster holds the MC3300x-G on a belt or waist band.

1. Secure the belt strap over the belt or waistband and snap into place.

Figure 135   Secure Belt Strap On Belt
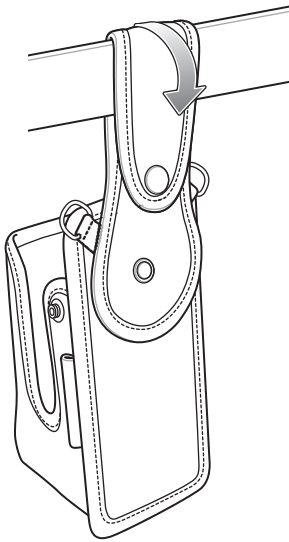
2. To insert the MC3300x-G, slide the mobile computer into the fabric holster with the screen facing the user.

Figure 136   Insert MC3300x-G
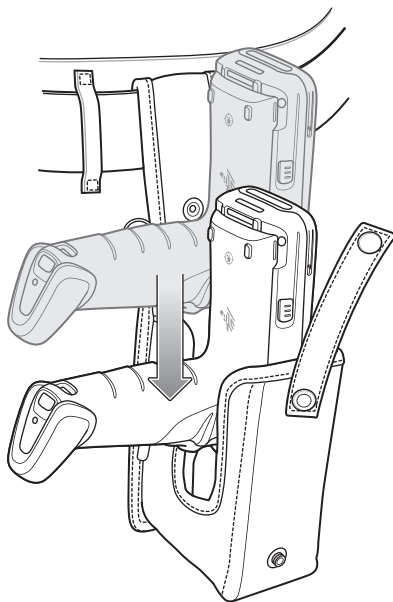
3. Secure the MC3300x-G with the restraining strap and place over the MC3300x-G to secure in place.

Figure 137   Secure with Strap
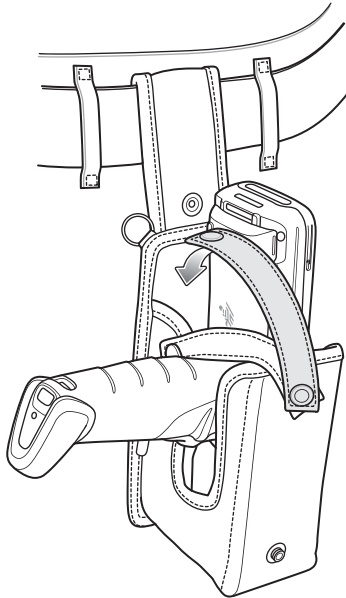
4. To remove the MC3300x-G, unsnap the restraining strap to release. Lift the MC3300x-G out of the fabric holster.

Using the Shoulder Strap

1. Connect the clips on the shoulder strap to the rings on the fabric holster.

2. Place the shoulder strap over your head and rest on your shoulder.

Figure 138   Shoulder Strap
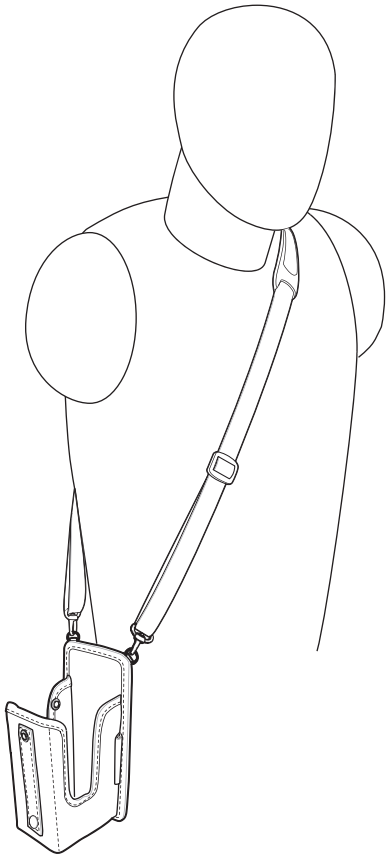
3. Lift the strap and insert the MC3300x-G into the holster.

4. Secure the strap to hold the MC3300x-G in place.

MC3300x-R/S Fabric Holster

The fabric holster provides a soft holder for the mobile computer. It consists of a fabric mobile computer holder, a detachable shoulder strap and a belt clip. See figures below to attach the fabric holster to a belt and shoulder strap.

Belt Clip

Attach the fabric holster to a belt or waist band.

Figure 139   Attach the Fabric Holster to a Belt
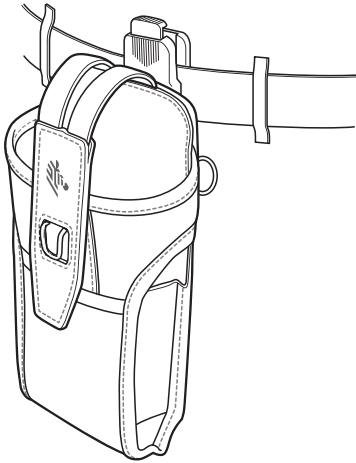
Shoulder Strap

Attach the fabric holster to a shoulder strap.

Figure 140   Attach the Fabric Holster to a Shoulder Strap

177
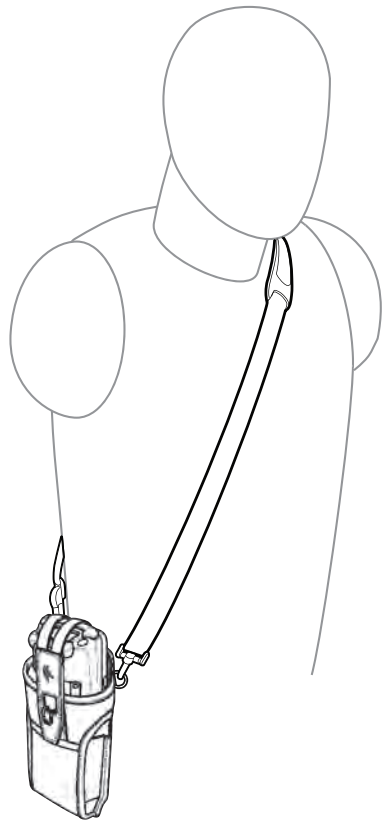
Using the Belt Clip

The fabric holster holds the MC3300x-R/S on a belt or waist band.

1. Secure the belt clip on the fabric holster, if it is not already attached.

Figure 141   Secure Belt Clip On Fabric Holster
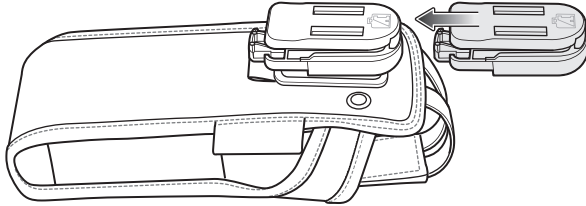
2. Secure the belt clip on the belt or waistband.

Figure 142   Secure Belt Clip On Belt
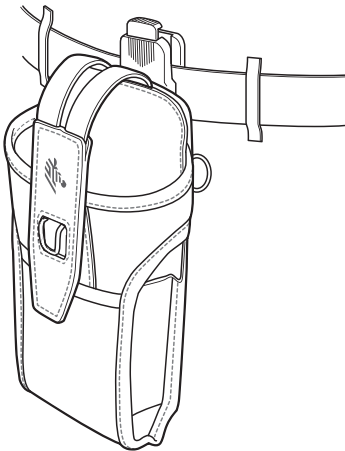
3. To insert the MC3300x-R/S, slide the mobile computer into the fabric holster with the screen facing the user.

Figure 143   Insert MC3300x-R/S
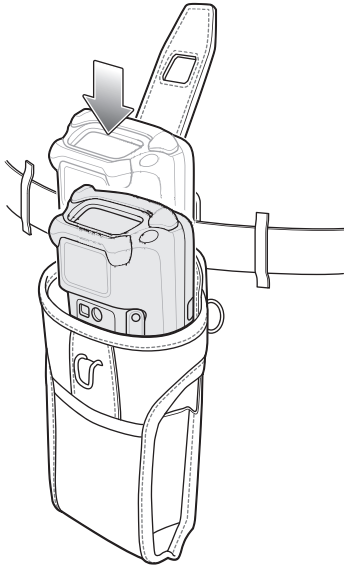
4. Secure the MC3300x-R/S with the restraining strap and place over the MC3300x-R/S to secure in place.

Figure 144   Secure with Strap
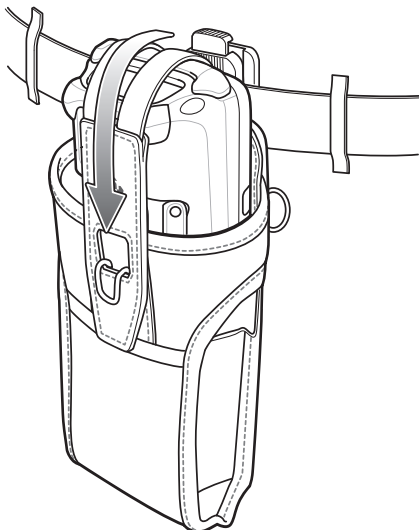
5. To remove the MC3300x-R/S, lift the restraining strap to release. Lift the MC3300x-R/S out of the fabric holster.

Using the Shoulder Strap

1. Connect the clips on the shoulder strap to the rings on the fabric holster.

2. Place the shoulder strap over your head and rest on your shoulder.

Figure 145   Shoulder Strap
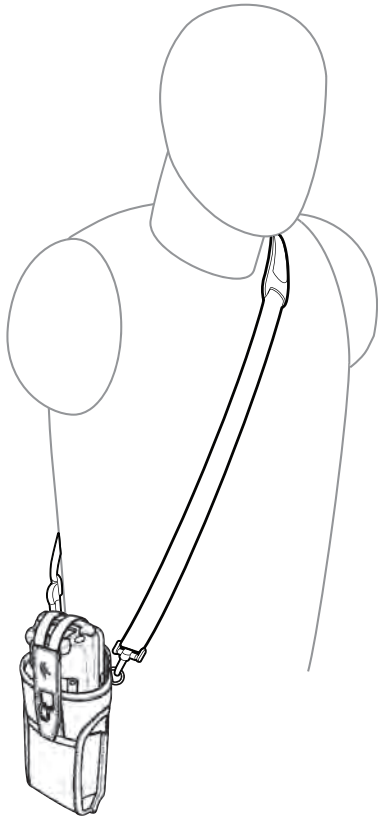
3. Lift the strap and insert the MC3300x-R/S into the holster.

4. Secure the strap to hold the MC3300x-R/S in place.

Un-powered Forklift Mount

The Un-powered Forklift Mount allows the user to place the MC3300x in a holder while installed on a forklift. However, it does not provide charging or communication to the terminal. The Forklift Mount can be installed on a square surface or roll bar of a forklift and supports portrait (vertical) orientation.

Figure 146   Forklift Mount
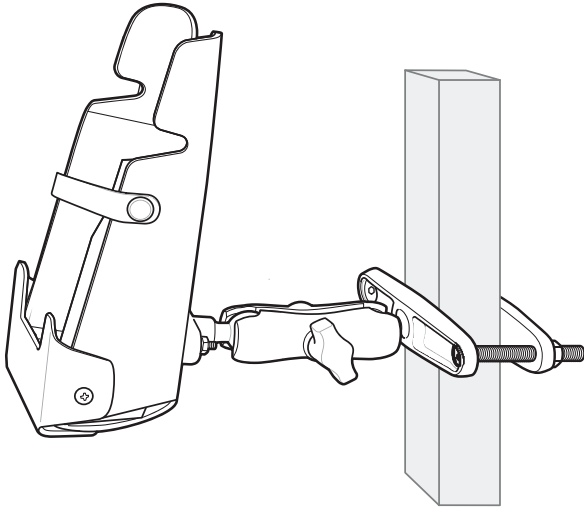
To use the MC3300x in the forklift mount holder:

1. Insert the MC3300x into the Forklift Mount Holder in an upright position.

Figure 147   Insert MC3300x
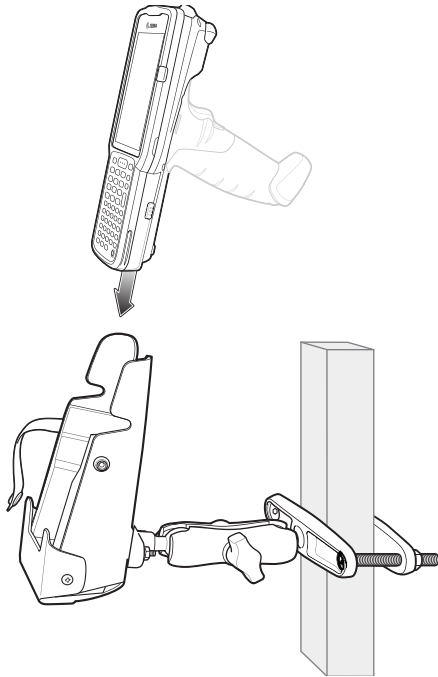
2. Secure the device with the rubber strap and snap into place.

Figure 148   Secure Device and Snap
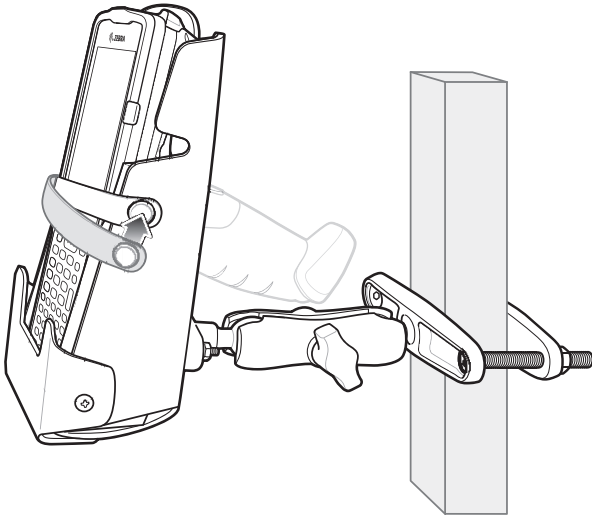
Replacement Hand Strap for MC3300x-G

To install the hand strap:

1. Thread the lanyard loop through the opening near the base of the trigger handle.

Figure 149   Insert Loop Through Handle Slot
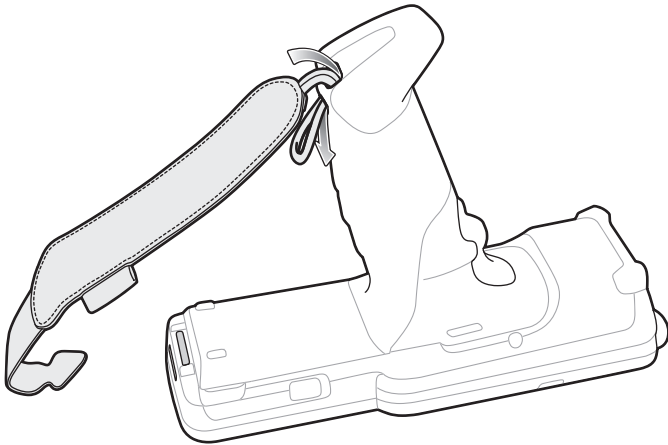
2. Insert the top end of the hand strap through the loop.

Figure 150   Thread Hand Strap Through Loop
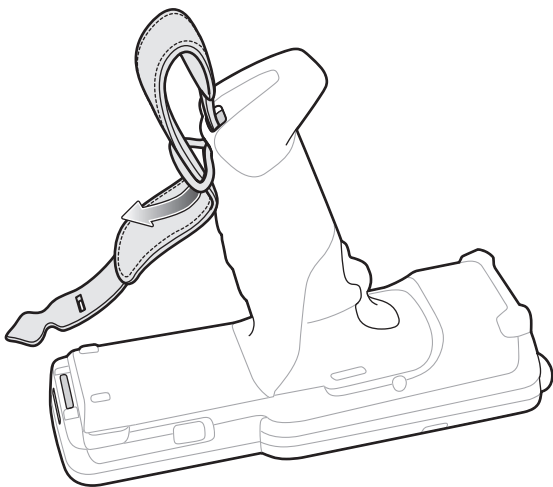
3. Thread the hand strap through the lanyard.

4. Pull the hand strap through the loop.

5. Thread the end of the hand strap with the tab through the slot on the bottom of the MC3300x-G.

Figure 151   Thread Tab Through Slot
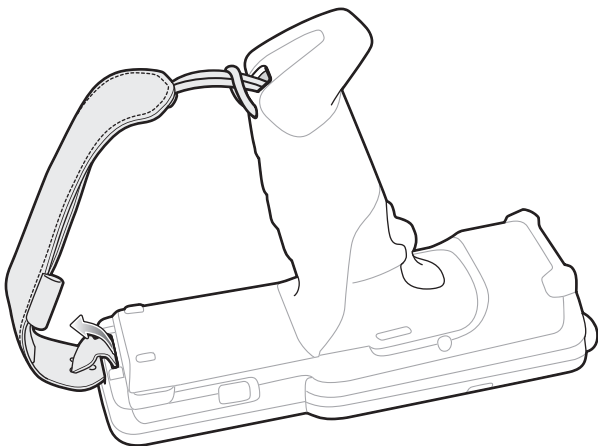
6. Slide the tab through the slit in the hand strap so that the tip of the tab is facing away from the MC3300x-G.

Replacement Hand Strap for MC3300x-R/S

To install the hand strap:

1. Thread the end of the hand strap with the tab through the slot toward the top of the MC3300x-R/S.

Figure 152   Thread Tab Through Top Slot
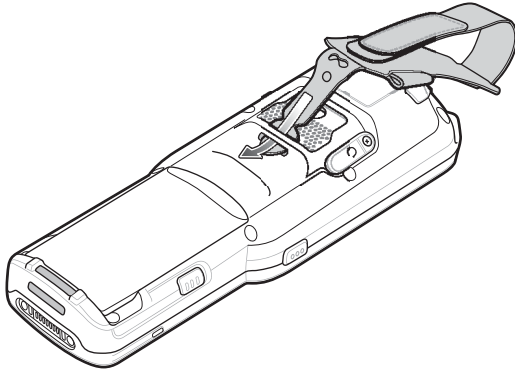
2. Slide the tab through the slit in the hand strap so that the tip of the tab is facing away from the MC3300x-R/S.

Figure 153   Slide Tab Through Slit
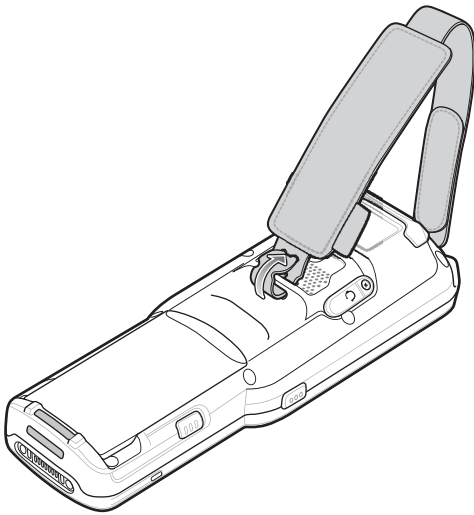
3. Thread the end of the hand strap with the velcro through the slot at the bottom of the MC3300x-R/S.

Figure 154   Thread Velcro Through Bottom Slot
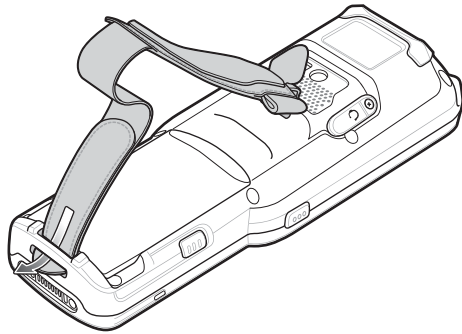
4. Pull the strap to the desired length and secure using the velcro.

Figure 155   Pull Strap and Secure Velcro
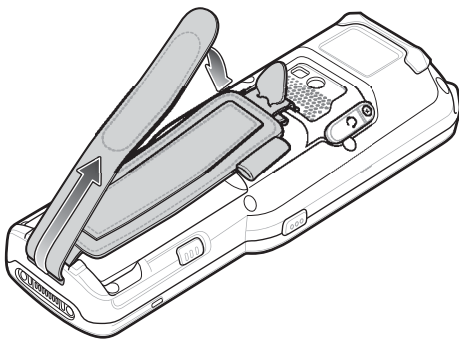
Lanyard

⚠ **WARNING:**   This accessory is not intended to be used with the MC33XX-G device.

The lanyard is an optional accessory for securing the MC33XX-R or MC33XX-S device to the user, which is comprised of multiple pieces. The lanyard can be worn using the cross-body strap, or it can be worn on the belt, after removing the cross-body strap.

Figure 156   Lanyard
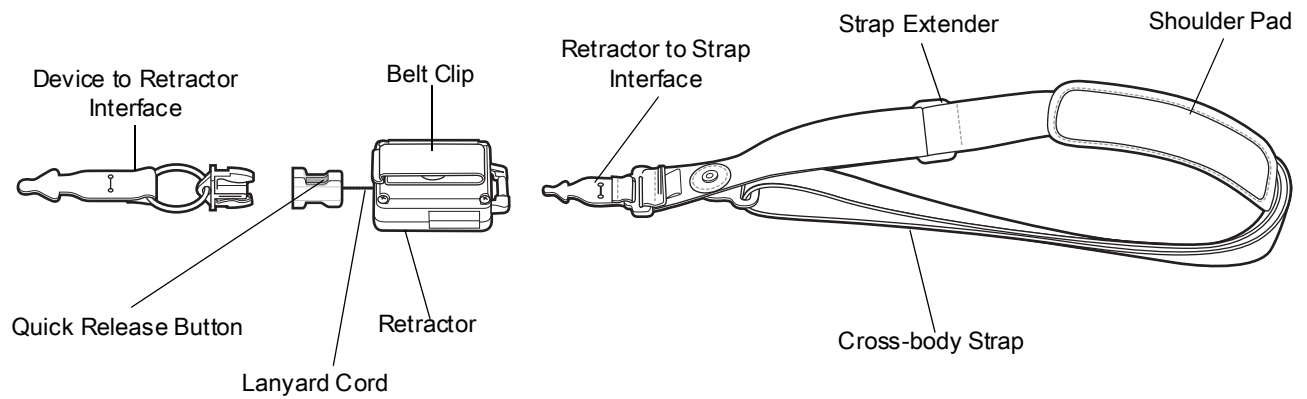
Install Lanyard on MC3300x

To install the lanyard on the MC3300x:

1. Thread the tab of the Device to Retractor Interface through the slot at the bottom of the MC3300x.

Figure 157   Thread Tab Through Slot
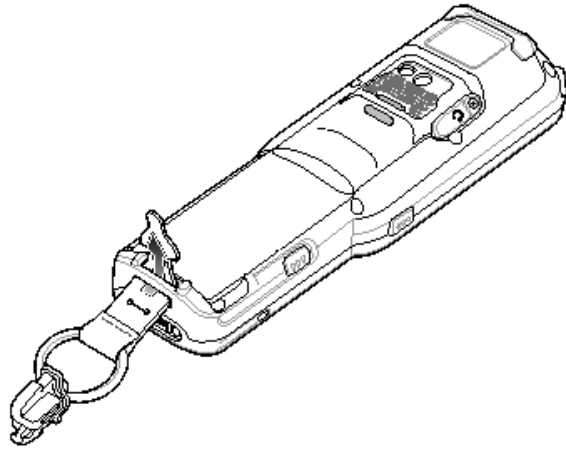
2. Slide the tab through the slit in the Device to Retractor Interface.

Figure 158   Slide Tab Through Slit
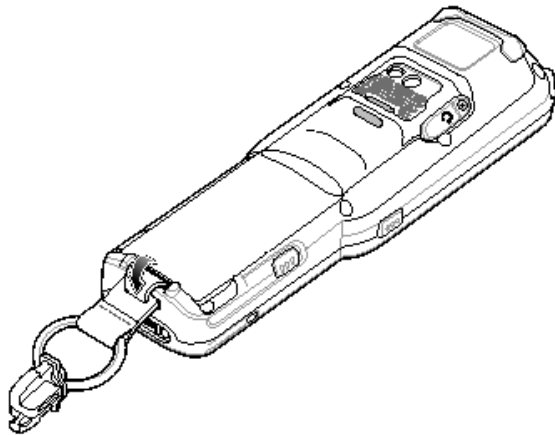
Using the Cross-body Strap

1. Place arm through strap and over the head to wear cross-body.

Figure 159   Cross-body Lanyard
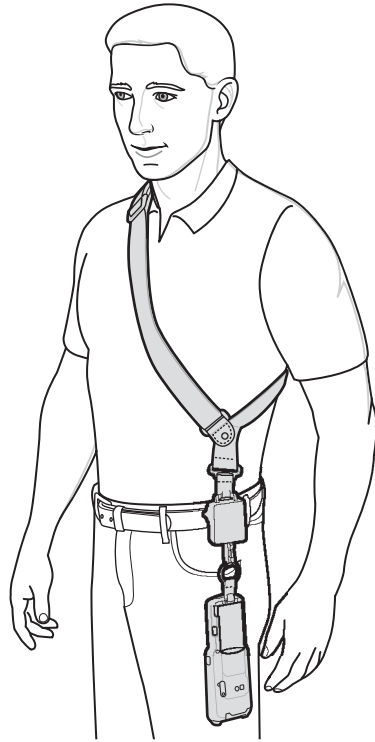
2. If needed, slide the Strap Extender to adjust the length of the Cross-body Strap to the desired length.

3. If needed, slide the Shoulder Pad along the Cross-body Strap to adjust the position of the Shoulder Pad for comfort.

Using the Belt Clip

To use the lanyard on a belt:

1. Detach the Cross-body Strap from the Retractor. To do this, unthread the tab of the Retractor to Strap Interface from the slot in the Retractor.

Figure 160   Remove Cross-body Strap
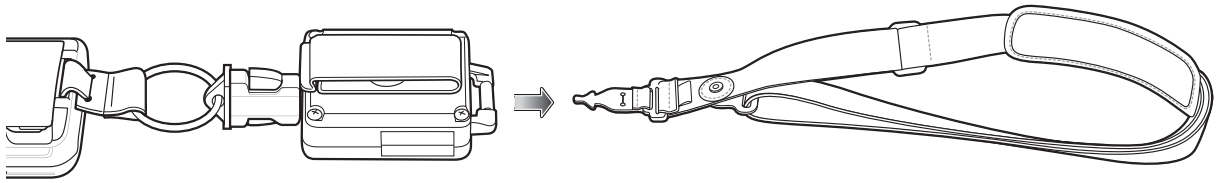
2. Place the Belt Clip on a belt or waistband.

Figure 161   Belt Clip Lanyard
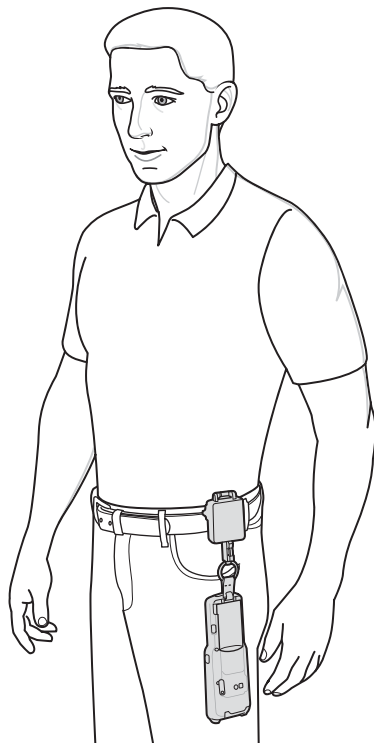
Charging the MC3300x with the Lanyard

To charge the MC3300x when using the lanyard:

1. Press the Quick Release Button on the Retractor.

2. Place the MC3300x in the charging cradle.

The Device to Retractor Interface remains attached to the MC3300x, while charging.

Application Deployment

Security

The device implements a set of security policies that determine whether an application is allowed to run and, if allowed, with what level of trust. To develop an application, you must know the security configuration of the device, and how to sign an application with the appropriate certificate to allow the application to run (and to run with the needed level of trust).

NOTE: Ensure the date is set correctly before installing certificates or when accessing secure web sites.

Secure Certificates

If the VPN or Wi-Fi networks rely on secure certificates, obtain the certificates and store them in the device's secure credential storage, before configuring access to the VPN or Wi-Fi networks.

If downloading the certificates from a web site, set a password for the credential storage. The device supports X.509 certificates saved in PKCS#12 key store files with a .p12 extension (if key store has a .pfx or other extension, change to .p12).

The device also installs any accompanying private key or certificate authority certificates contained in the key store.

Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the microSD card or the device's internal memory. See USB Communication for information about connecting the device to a host computer and copying files.

2. Go to **Settings**.

3. Touch **Security & location** > **Advanced** > **Encryption & credentials**.

4. Touch **Install from storage**.

5. Navigate to the location of the certificate file.

6. Touch the filename of the certificate to install.

7. If prompted, enter the password for credential storage. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.

8. If prompted, enter the certificate's password and touch **OK**.

9. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.

10. Touch **OK**.

The certificate can now be used when connecting to a secure network. For security, the certificate is deleted from the microSD card or internal memory.

Configuring Credential Storage Settings

1. Go to **Settings**.

2. Touch **Security & location > Encryption & credentials**.
   - **Trusted credentials** - Touch to display the trusted system and user credentials.
   - **Install from storage** - Touch to install a secure certificate from the microSD card or internal storage.
   - **Clear credentials** - Deletes all secure certificates and related credentials.

License Manager

License Manager is an Android application and is offered to customers having Back-Office Server, Relay/Proxy Server and Local/On-Premise Server infrastructures for manual license activation of Zebra Technologies software products. This then enables the corresponding software or device functionality. The application also shows the list of active licenses on the device along with the products and their features and versions. All the license rights displayed in the application are available for acquisition on the device.

Use License Manager to manage software licenses on the MC33XX. The License Manager administers the software licenses on a device, allowing an administrator or application on the device to control the usability of software features that require licensing. Software components can be made usable, unusable or feature-limited based on the license on the device. If a component requires licensing, the absence of a valid license will limit or prevent its functionality.

Android Versions Supported

- KitKat
- Lollipop
- Marshmallow
- Nougat
- Oreo

Requirements

- License Manager and LicenseMgrService applications pre-installed on the device.
- Network Connection
- Back-Office Server, Relay/Proxy Server or Local/On-Premise Server infrastructure setup

Start Application

To start License Manager:

1. On the Home screen, swipe up from the bottom of the screen.

2. Touch ![icon] **License Manager**.

   The application starts and displays the following License Manager Home screen, when there are no licenses currently active on the device.

Figure 162   License Manager Home Screen - Without Licenses
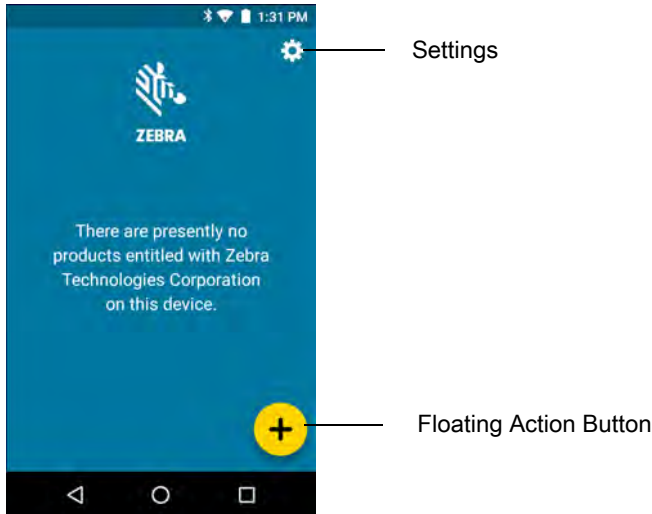
The application starts and displays the following License Manager Home screen, when there are licenses currently active on the device.

Figure 163   License Manager Home Screen - With Licenses
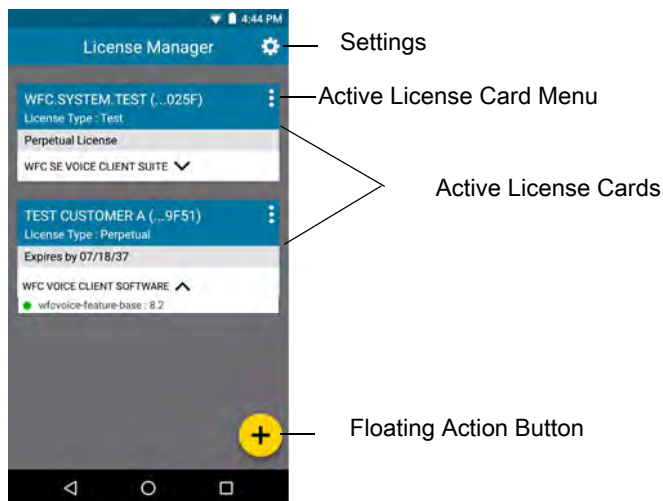
Active License Display

All licenses currently active on the device display in the form of cards on the License Manager Home screen. Each card corresponds to an active license. Each license on the License Manager Home screen contains the following information:

First Row - Includes the name of the organization who purchased the license along with the last four digits of the activation ID used for activating the license.

Second Row - Includes the license type. Valid license types:

- **Perpetual**
- **Permanent**
- **Trial License**
- **Test**

Third Row - Includes the expiration date of the license in the format MM/DD/YY. If the license type is Perpetual/Permanent, **Expires Never** displays.

Remaining Rows - The rows below the expiration date include a list of products followed by an arrow at the end of each row which enables you to expand each product to view the list of features activated for the product. Each row under a product includes a list of features and their version numbers, which can be used for acquisition on the device.

Activate License

To activate a license for any Zebra Technologies software products:

1. On the **MC33XX Home** screen, swipe up from the bottom of the screen.

2. Touch ![icon] **License Manager**.

   The **License Manager Home** screen displays.

3. On the **License Manager Home** screen, touch the **Floating Action** button.

   The **Activate License** screen displays.

Figure 164   Activate License Screen
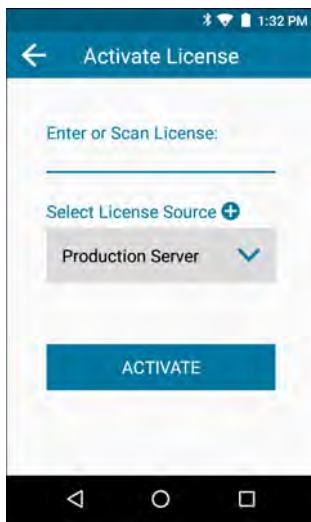
4. Enter or scan a license.

   Either manually enter a valid activation ID or scan a valid license.

5. Touch **Select License Source**. Choose an existing default license source (Back-Office Servers) or add a new Custom (Proxy/Relay Server) and Local (On-Premise Server) license source.

   The **Source** selection screen displays.

Figure 165   Source Selection Screen
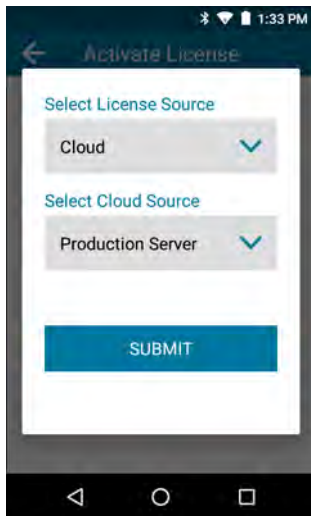
6. Select **License Source**. This drop-down list includes all the license sources available on the device. A valid license source must be selected. This field usually indicates the name of the server for any of the user-added license sources. There are three default license sources available.

- **Cloud**
- **Local Server**
- **Offline**

The user has the ability to add a new Custom Server or a new Local Server. See Add License Source on page 195. All license sources (Custom/Local) added by the user are read only. All the license sources added by the user are displayed below the three default options.

Figure 166   Select License Source Options
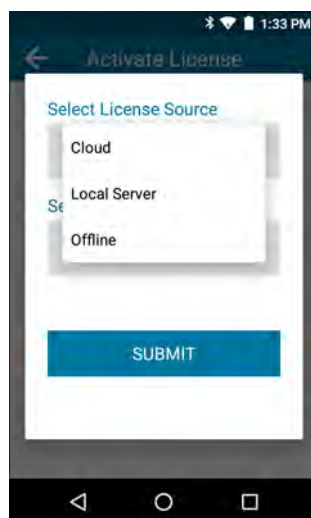
7. Select **Cloud Source**. This drop-down list includes the default servers (Production or UAT) and custom servers (Relay/Proxy Server). This field displays only when the **Select License Source** field is set to **Cloud**. A valid cloud source must be selected. When selecting **Custom Server**, the user is prompted to

194

add a new license source. The license source added corresponds to a custom relay/proxy server set up by the customer.

- **Production Server**
- **UAT Server**
- **Custom Server**

Figure 167   Select Cloud Source Options
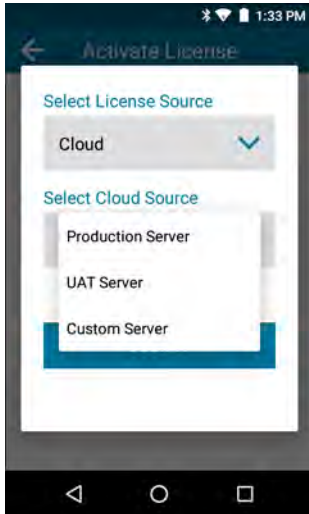
8. Enter the **URL** of the license source. This field only displays when the user is given the option to add a new license source for **Custom Server** and **Local Server**. This field is visible while viewing any user-added license source which will be read-only.

9. Enter **Name**. This field only displays when the user is given the option to add a new license source for **Custom Server** and **Local Server**. A valid unique name of the license source must be entered. This field is visible while viewing any user-added license source. The name added in this field is added to the list of license sources saved on the device.

10. Touch **Submit**.

The application validates the information and connects to the selected License Source, and displays whether the license activation was successful or not.

If the license activation is successful, the activated license information displays in the form of a card on the **License Manager Home** screen.

All of the license rights displayed on the **License Manager Home** screen are available for acquisition on the device.

Add License Source

The user has the option to add a new Custom Server or a Local Server license source. New license sources can be added from the **Activate License** screen or from the **License Source Settings** screen.

To add a new license source from the **Activate License** screen:

1. Add a **License Source** (Local or Custom):

    Local: From the **Select License Source** drop-down list, select **Local Server** to add a local license source.

    Custom: From the **Select License Source** drop-down list, select **Cloud** and from the **Select Cloud Source** drop-down list, select **Custom Server**.

Figure 168   Select License Source Screen
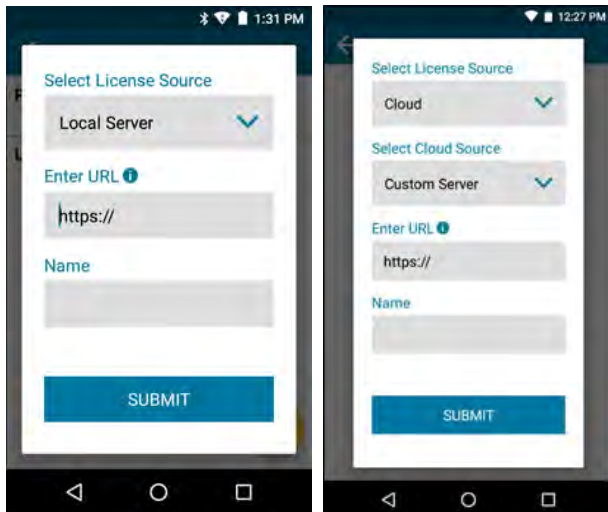
2. Enter a valid server URL and a unique name to identify the license source.

3. Touch **Submit**.

   All the valid license sources added by the user (Custom/Local) are available for selection in the **Select License Source** list in the **License Source** screen while activating a license. All the license sources also display in the **License Sources Settings** screen.

   NOTE: All license sources (Custom and Local) added by the user are read only. A maximum of ten license sources can be saved on the device at a time, including the default Production and UAT license sources. Therefore, the user can add a maximum of eight license sources (Custom license source only, Local license source only, or a combination of both).

Refresh a License

To refresh a license which is currently active on the device:

1. On the **MC33XX Home** screen, swipe up from the bottom of the screen.

2. Touch ⊡ **License Manager**.

   The **License Manager Home** screen displays.

3. Activate a license if no licenses are currently active on the device. For more information, see Activate License on page 193.

   Once one or more licenses are currently active on the device, the user can see the **License Manager Home** screen with a list of cards.

4. Choose the license that needs to be refreshed and touch ⋮ .

5. Touch **Refresh License**.

   A request is sent to the server to refresh the selected license. Once the license is successfully refreshed, all the information in the card corresponding to the license is updated.

196

Settings

To access License Manager Settings:

1. On the **MC33XX Home** screen, swipe up from the bottom of the screen.

2. Touch **License Manager**.

   The **License Manager Home** screen displays.

3. Touch **Settings**.

Figure 169   Settings Screen

Notifications Settings

Use Notifications to set whether you want to receive push notifications and a reminder for the license expirations.

Figure 170   Notifications
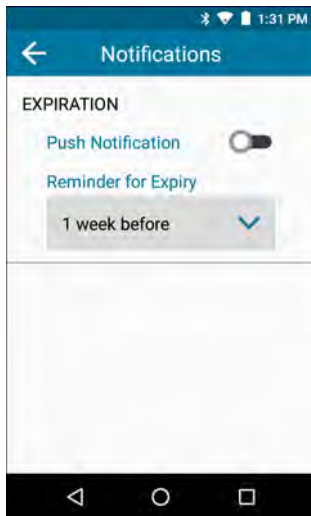
Push Notification - Toggle the switch to the ON position, to receive notifications on the device for license expiry.

Reminder for Expiry - Touch the drop-down list, to set the time period before which the user is notified of license expiry.

- **1 week before** (default)
- **2 weeks before**
- **3 weeks before**
- **4 weeks before**

Once the **Push Notification** switch is set and the desired time period is chosen, a notification appears in the Status Bar if any licenses currently active on the devise is going to expire within the time period set. The user is notified of the license expiry within the time frame and the product name and activation ID displays in the notification. The user can click on the notification from the Notifications pull-down which redirects the user to the **License Manager Home** screen.

License Sources Settings

All the license sources available on the device can be viewed by selecting the **License Sources** option on the Settings screen. This screen can also be opened by selecting License Source from the menu on the License Manager Home screen.

Figure 171   License Source Screen
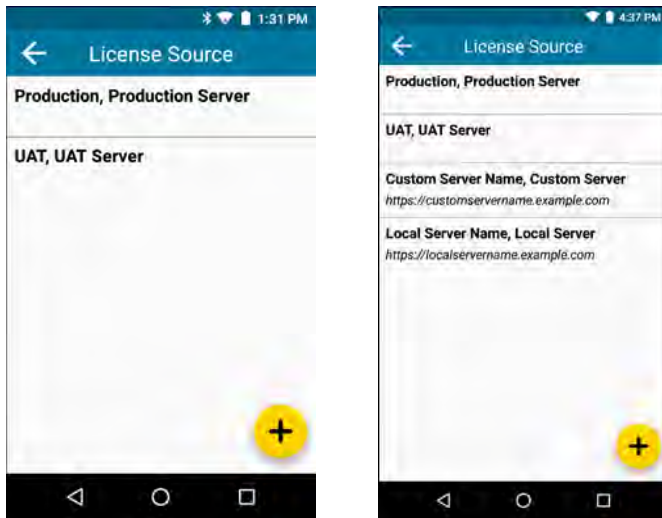
The first two items in the License Source screen are the default license sources:

- **Production Server**
- **UAT Server**

These two license sources are followed by user-added license sources.

Add License Source in Settings

The user can add a new Custom Server or a Local Server license source. New license sources can be added from the **Activate License** screen or from the **License Source Settings** screen.

To add a new license source from the **License Source Settings** screen:

1. On the **MC33XX Home** screen, swipe up from the bottom of the screen.

2. Touch **License Manager**.

   The **License Manager Home** screen displays.

3. Touch **Settings**.

4. Touch **License Sources**.

5. Touch the **Floating Action** button (plus icon) on the bottom right corner of the **License Source** screen.

6. Add a **License Source** (Local or Custom):

   Local: From the **Select License Source** drop-down list, select **Local Server** to add a local license source.

   Custom: From the **Select License Source** drop-down list, select **Custom Server** to add a custom license source.

Figure 172   Select License Source Screen
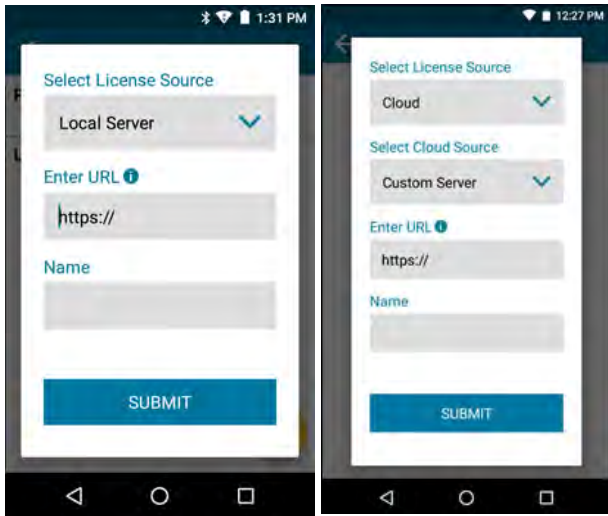
7. Enter a valid server URL and a unique name to identify the license source.

8. Touch **Submit**.

The recently added license source on the **Settings** screen is automatically selected as the current license source in the **Activate License** screen. All the valid license sources added by the user (Custom/Local) are available for selection in the **Select License Source** list in the **License Source** screen while activating a license.

> **NOTE:** All license sources (Custom and Local) added by the user are read only. A maximum of ten license sources can be saved on the device at a time, including the default Production and UAT license sources. Therefore, the user can add a maximum of eight license sources (Custom license source only, Local license source only, or a combination of both).

About Settings

The information that displays on the About screen is read only and depends on the device and the version of the License Manager application installed on the device.

Figure 173   About Screen

Device ID - Displays the unique serial number of the device on which License Manager is installed.

License Manager Version - Displays the version of License Manager installed on the device.

License Agent Version - Displays the version of the License Agent installed on the device.

Development Tools

Android Application Development

Development Workstation

Android development tools are available at developer.android.com.

To start developing applications for the device, download Android Studio. Development can take place on a Microsoft® Windows®, Mac® OS X®, or Linux® operating system.

Applications are written in the Java language, but compiled and executed in the Dalvik virtual machine. Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

Android Studio contains a full featured IDE as well as SDK components required to develop Android applications.

Target Device

Open the **Developer options** screen to set development related settings.

By default, the Developer Options are hidden. To un-hide the developer options, go to **Settings**.

Touch **System > About device**. Scroll down to **Build number**. Tap **Build number** seven times until **You are now a developer appears**.

Touch **System > Developer options**. Slide the switch to the **ON** position to enable developer options.

EMDK for Android

EMDK for Android provides developers with a comprehensive set of tools to easily create powerful line-of-business applications for enterprise mobile computing devices. It's designed for Google's Android SDK and Android Studio, and includes class libraries, sample applications with source code, and all associated documentation to help your applications take full advantage of what Zebra devices have to offer.

The kit also delivers Profile Manager, a GUI-based device configuration tool providing exclusive access to the Zebra MX device management framework. This allows developers to configure Zebra devices from within their applications in less time, with fewer lines of code and with fewer errors.

For more information go to: techdocs.zebra.com.

StageNow

StageNow is Zebra's next-generation Android Staging Solution built on the MX platform. It allows quick and easy creation of device profiles, and can deploy to devices simply by scanning a bar code, reading a tag, or playing an audio file.

The StageNow Staging Solution includes the following components:

- The StageNow Workstation tool installs on the staging workstation (host computer) and lets the administrator easily create staging profiles for configuring device components, and perform other staging actions such as checking the condition of a target device to determine suitability for software upgrades or other activities. The StageNow Workstation stores profiles and other created content for later use.

- The StageNow Client resides on the device and provides a user interface for the staging operator to initiate staging. The operator uses one or more of the desired staging methods (print and scan a bar code, read an NFC tag or play an audio file) to deliver staging material to the device.

For more information go to: techdocs.zebra.com.

ADB USB Setup

To use the ADB, install the USB driver. This assumes that the development SDK has been installed on the host computer. Go to developer.android.com/sdk/index.html for details on setting up the development SDK.

ADB driver for Windows and Linux are available on the Zebra Support Central web site at www.zebra.com/support. Download the ADB and USB Driver Setup package. Following the instructions with the package to install the ADB and USB drivers for Windows and Linux.

Enabling USB Debugging

By default, USB debugging is disabled. To enable USB debugging:

1. Go to **Settings**.

2. Touch **System > About phone**.

3. Scroll down to **Build number**.

4. Tap **Build number** seven times. The message **You are now a developer!** appears.

5. Touch ◁.

6. Touch **Developer options**.

7. Slide the **USB debugging** switch to the **ON** position.

8. Touch **OK**.

9. Connect the device to the host computer using the Rugged Charge/USB Cable.

   The **Allow USB debugging?** dialog box appears on the device.

10. On the device, touch **OK**.

11. On the host computer, navigate to the `platform-tools` folder.

12. Type `adb devices`.

    The following displays:

    `List of devices attached`

    `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

13. Touch ◯.

Application Installation

After an application is developed, install the application onto the device using one of the following methods:

- USB connection, see Installing Applications Using the USB Connection.
- Android Debug Bridge, see Installing Applications Using the Android Debug Bridge.
- microSD Card, see Installing Applications Using a microSD Card.
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

Installing Applications Using the USB Connection

CAUTION: When connecting the device to a host computer and mounting the microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

1. Connect the device to a host computer using the Rugged Charge/USB cable.
2. Pull down the Notification panel and touch **USB for Charging**.
3. Touch **Transfer files**.
4. On the host computer, open a **Files** application.
5. On the host computer, copy the application .apk file from the host computer to the device.

CAUTION: Carefully follow the host computer's instructions to unmount the microSD card and disconnect USB devices correctly to avoid losing information.

6. Disconnect the device from the host computer.
7. Swipe the screen up and select 🔵 to view files on the microSD card or Internal Storage.
8. Locate the application .apk file.
9. Touch the application file.
10. Touch **Continue** to install the app or **Cancel** to stop the installation.
11. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
12. Touch **Open** to open the application or **Done** to exit the installation process. The application appears in the App list.

Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.

CAUTION: When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Ensure that the ADB drivers are installed on the host computer. See ADB USB Setup.

1. Connect the device to a host computer using USB. See USB Communication.
2. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
3. Touch **System > Developer options**.

4. Slide the switch to the **ON** position.

5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.

6. Touch **OK**.

7. On the host computer, open a command prompt window and use the adb command:

   `adb install <application>`

   where: <application> = the path and filename of the apk file.

8. Disconnect the device from the host computer. See USB Communication.

Installing Applications Using a microSD Card

⚠️ **CAUTION:** When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

1. Connect the device to a host computer using USB. See USB Communication.

2. Copy the application APK file from the host computer to the microSD card.

3. Remove the microSD card from the host computer.

4. Press and hold the Power button until the menu appears.

5. Touch **Power off**.

6. Press the two battery latches in.

7. Lift the battery from the device.

8. Lift the access door.

9. Insert the microSD card.

10. Replace the access door.

11. Insert the battery, bottom first, into the battery compartment in the back of the device.

12. Press the battery down until the battery release latches snap into place.

13. Press and hold the Power button to turn on the device.

14. Swipe the screen up and select 🔵 to view files on the microSD card.

15. Touch ≡ > **SD card**.

16. Locate the application .apk file.

17. Touch the application file.

18. Touch **Continue**. to install the app or **Cancel** to stop the installation.

19. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.

20. Touch **Open** to open the application or **Done** to exit the installation process. The application appears in the App list.

Uninstalling an Application

To uninstall an application:

1. Go to **Settings**.

2. Touch **Apps & notifications**.

3. Touch **See all apps** to view all apps in the list.

4. Scroll through the list to the app.

5. Touch the app. The **App info** screen appears.

6. Touch **Uninstall**.

7. Touch **OK** to confirm.

Performing a System Update

System Update packages can contain either partial or complete updates for the operating system. Zebra distributes the System Update packages on the Zebra Support & Downloads web site. Perform system update using either a microSD card or using ADB.

Downloading the System Update Package

To download the system update package:

1. Go to the Zebra Support & Downloads web site, www.zebra.com/support.

2. Download the appropriate System Update package to a host computer.

Using microSD Card

1. Copy the System Update zip file to the root of the microSD card.
    - Copy the zip file to a microSD card using a host computer (see USB Communication for more information), and then installing the microSD card into the device (see Replacing the microSD Card for more information).
    - Connect the device with a microSD card already installed to the host computer, and copy zip file to the microSD card. See USB Communication on page 46 for more information. Disconnect the device from the host computer.

2. Press and hold the Power button until the menu appears.

3. Touch **Reboot**.

4. Touch **OK**. The device resets.

5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.

6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.

7. Press the Power button.

8. Use the Volume Up and Volume Down buttons to navigate to the System Update file.

9. Press the Power button. The System Update installs and then the device returns to the Recovery screen.

10. Press the Power button to reboot the device.

NOTE: If installing GMS software on a device that had Non-GMS software or Non-GMS software on a device that had GMS software, perform a Factory or Enterprise reset (retains enterprise data).

Using ADB

To update the system using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.

2. Connect the cable or cradle to the host computer.

3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

4. Touch **System > Developer options**.

5. Slide the switch to the **ON** position.

6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.

7. Touch **OK**.

8. On the host computer, open a command prompt window and use the adb command:

   `adb devices`

   The following displays:

   `List of devices attached`

   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

9. Type:

   `adb reboot recovery`

10. Press Enter. The System Recovery screen appears.

11. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

12. Press the Power button.

13. On the host computer command prompt window type:

   `adb sideload <file>`

   where: <file> = the path and filename of the zip file.

14. Press Enter. The System Update installs (progress appears as percentage in the Command Prompt window) and then the Recovery screen appears.

15. Press the Power button to reboot the device.

NOTE: If installing GMS software on a device that had Non-GMS software or Non-GMS software on a device that had GMS software, perform a Factory or Enterprise reset (retains enterprise data).

Verify System Update Installation

To check that the system update installed properly:

1. Go to **Settings**.

2. Touch **System** > **About phone**.

3. Scroll down to **Build number**.

4. Ensure that the build number matches the new system update package file number.

Performing an Enterprise Reset

An Enterprise Reset erases all user data in the `/data` partition, including data in the primary storage locations (`/sdcard` and emulated storage).

Before performing an Enterprise Reset, provision all necessary configuration files and restore after the reset.

Perform Enterprise Reset using either a microSD card or using ADB.

Downloading the Enterprise Reset Package

To download the system update package:

1. Go to the Zebra Support & Downloads web site, www.zebra.com/support.

2. Download the Enterprise Reset file to a host computer.

Using microSD Card

1. Copy the Enterprise Reset zip file to the root of the microSD card.
   - Copy the zip file to a microSD card using a host computer (see USB Communication for more information) and then installing the microSD card into the device (see Replacing the microSD Card for more information).
   - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See USB Communication for more information. Disconnect the device from the host computer.

2. Press and hold the Power button until the menu appears.

3. Touch **Reboot**.

4. Touch **OK**. The device resets.

5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.

6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.

7. Press the Power button.

8. Use the Volume Up and Volume Down buttons to navigate to the System Update file.

9. Press the Power button. The Enterprise Reset occurs and then the device returns to the Recovery screen.

10. Press the Power button.

Using ADB

To perform an Enterprise Reset using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.

2. Connect the cable or cradle to the host computer.

3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

4. Touch **System** > **Developer options**.

5. Slide the switch to the **ON** position.

6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.

7. Touch **OK**.

8. On the host computer, open a command prompt window and type:

   `adb devices`.

   The following displays:

   `List of devices attached`

   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

9. Type:

   `adb reboot recovery`

10. Press Enter. The System Recovery screen appears.

11. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

12. Press the Power button.

13. On the host computer command prompt window type:

    `adb sideload <file>`

    where: <file> = the path and filename of the zip file.

14. Press Enter. The Enterprise Reset package installs and then the Recovery screen appears.

15. Press the Power button to reboot the device.

Performing a Factory Reset

A Factory Reset erases all data in the **/data** and **/enterprise** partitions in internal storage and clears all device settings. A Factory Reset returns the device to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See Performing a System Update for more information.

Downloading the Factory Reset Package

To download the Factory Reset package:

1. Go to the Zebra Support & Downloads web site, www.zebra.com/support.

2. Download the appropriate Factory Reset file to a host computer.

Using microSD Card

1. Copy the Factory Reset zip file to the root of the microSD card.
   - Copy the zip file to a microSD card using a host computer (see USB Communication for more information) and then installing the microSD card into the device (see Replacing the microSD Card for more information).
   - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See USB Communication for more information. Disconnect the device from the host computer.

2. Press and hold the Power button until the menu appears.

3. Touch **Reboot**.

4. Touch **OK**. The device resets.

5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.

6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.

7. Press the Power button.

8. Use the Volume Up and Volume Down buttons to navigate to the Factory Reset file.

9. Press the Power button. The Factory Reset occurs and then the device returns to the Recovery screen.

10. Press the Power button.

Using ADB

To perform an Factory Reset using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.

2. Connect the cable or cradle to the host computer.

3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

4. Touch **System > Developer options**.

5. Slide the switch to the **ON** position.

6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.

7. Touch **OK**.

8. On the host computer, open a command prompt window and use the adb command:

   `adb reboot recovery`

9. Press Enter. The System Recovery screen appears.

10. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

11. Press the Power button.

12. On the host computer, open a command prompt window and use the adb command:

    `adb devices`.

    The following displays:

    `List of devices attached`

    `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

13. Type:

    `adb reboot recovery`

14. Press Enter. The System Recovery screen appears.

15. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

16. Press the Power button.

17. On the host computer command prompt window type:

    `adb sideload <file>`

    where: <file> = the path and filename of the zip file.

18. Press Enter. The Factory Reset package installs and then the Recovery screen appears.

19. Press the Power button to reboot the device.Replace the top cover.

Storage

The device contains the following types of file storage:

- Random Access Memory (RAM)
- Internal storage
- External storage (microSD card) or
- Enterprise folder.

Random Access Memory

Executing programs use RAM to store data. Data stored in RAM is lost upon a reset. The operating system manages how applications use RAM. It only allows applications and component processes and services to use RAM when required. It may cache recently used processes in RAM, so they restart more quickly when opened again, but it will erase the cache if it needs the RAM for new activities.

1. To view the amount of free and used memory, go to **Settings**.

2. Touch **System** > **Developer options** > **Memory**.

The screen displays the amount of used and free RAM.

- **Performance** - Indicates memory performance.
- **Total memory** - Indicates the total amount of RAM available.
- **Average used (%)** - Indicates the average amount of memory (as a percentage) used during the period of time selected (default - 3 hours).

- **Free** - Indicates the total amount of unused RAM.
- **Memory used by apps** - Touch to view RAM usage by individual apps.

Internal Storage

The device has internal storage. The internal storage content can be viewed and files copied to and from when the device is connected to a host computer. Some applications are designed to be stored on the internal storage rather than in internal memory.

To view the used and available space on the internal storage:

1. Go to **Settings**.

2. Touch **Storage**.

- **Internal Storage** - Displays the total amount of space on internal storage and amount used.

Touch **Internal shared storage** to display a the amount of storage used by apps, photos, videos, audio and other files.

External Storage

The device can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the device is connected to a host computer.

To view the used and available space on the microSD card:

1. Go to **Settings**.

2. Touch **Storage**.

Portable storage displays the total amount of space on the installed microSD card and the amount used.

To unmount the microSD card, touch ▲.

Touch **SD card** to view the contents of the card.

Formatting a microSD Card or USB Drive as Portable Storage

To format an installed microSD card or USB drive as portable storage:

1. Touch **SD card**.

2. Touch ⋮ > **Storage settings**.

3. Touch **Format**.

4. Touch **ERASE & FORMAT**.

5. Touch **DONE**.

Formatting a microSD Card as Internal Memory

You can format a microSD card as internal memory to increase the actual amount of the device's internal memory. Once formatted, the microSD card can only be read by this device. To format an installed microSD card as internal memory:

1. Touch **SD card**.

2. Touch **⋮** > **Storage settings**.

3. Touch **Format as internal**.

4. Touch **ERASE & FORMAT**.

5. Touch **DONE**.

Enterprise Folder

The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 MB (formatted). Applications can persist data after an Enterprise Reset by saving data to the enterprise/user folder. The folder is ext4 formatted and is only accessible from a host computer using ADB or from an MDM.

App Management

Apps use two kinds of memory: storage memory and RAM. Apps use storage memory for themselves and any files, settings, and other data they use. They also use RAM when they are running.

1. Go to **Settings**.

2. Touch **Apps & notifications**.

3. Touch **See all XX apps** to view all apps on the device.

4. Touch **⋮** > **Show system** to include system processes in the list.

5. Touch an app, process, or service in the list to open a screen with details about it and, depending on the item, to change its settings, permissions, notifications and to force stop or uninstall it.

Viewing App Details

Apps have different kinds of information and controls, but commonly include:

*   **Force stop** - stop an app.
*   **Disable** - disable an app.
*   **Uninstall** - remove the app and all of its data and settings from the device. See Uninstalling an Application for information about uninstalling apps.
*   **Storage** - lists how much information is stored, and includes a button for clearing it.
*   **Data usage** - provides information about data (Wifi) consumed by an app.
*   **Permissions** - lists the areas on the device that the app has access to.
*   **Notifications** - set the app notification settings.
*   **Open by default** - clears If you have configured an app to launch certain file types by default, you can clear that setting here.
*   **Battery** - lists the amount of computing power used by the app.
*   **Memory** - lists the average app memory usage.
*   Advanced
    *   **Draw over other apps** - allows an app to display on top of other apps.

212

Managing Downloads

Files and apps downloaded using the Browser or Email are stored on the microSD card or Internal storage in the Download directory. Use the Downloads app to view, open, or delete downloaded items.

1. Swipe the screen up and touch ⬤.

2. Touch ≡ > **Downloads**.

3. Touch and hold an item, select items to delete and touch 🗑. The item is deleted from the device.

Maintenance and Troubleshooting

Maintaining the Device

For trouble-free service, observe the following tips when using the device:

*   In order to avoid scratching the screen, use the supplied stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the device screen.
*   The touch-sensitive screen of the device is glass. Do not drop the device or subject it to strong impact.
*   Protect the device from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
*   Do not store the device in any location that is dusty, damp, or wet.
*   Use a soft lens cloth to clean the device. If the surface of the device screen becomes soiled, clean it with a soft cloth moistened with an approved cleanser. For a list of approved cleansers, see Approved Cleanser Active Ingredients.
*   Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.
*   A screen protector is applied to the device. Zebra recommends using this to minimize wear and tear. Screen protectors enhance the usability and durability of touch screen displays. Benefits include:
    *   Protection from scratches and gouges
    *   Durable writing and touch surface with tactile feel
    *   Abrasion and chemical resistance
    *   Glare reduction
    *   Keeping the device's screen looking new
    *   Quick and easy installation.

Battery Safety Guidelines

*   The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
*   Follow battery usage, storage, and charging guidelines found in this guide.
*   Improper battery use may result in a fire, explosion, or other hazard.
*   To charge the mobile device battery, the ambient battery and charger temperatures must be between +32ºF and +104ºF (0ºC and +40ºC)

- Do not use incompatible batteries and chargers, including non-Zebra batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact the Global Customer Support Center.

- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.

- To enable authentication of an approved battery, as required by IEEE1725 clause 10.2.1, all batteries will carry a hologram. Do not fit any battery without checking it has the authentication hologram.

- Do not disassemble or open, crush, bend or deform, puncture, or shred battery.

- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.

- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.

- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.

- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.

- Battery usage by children should be supervised.

- Please follow local regulations to properly dispose of used re-chargeable batteries.

- Do not dispose of batteries in fire.

- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with water for 15 minutes and seek medical advice.

- If you suspect damage to your equipment or battery, contact Customer Support to arrange for inspection.

Cleaning Instructions

CAUTION: Always wear eye protection.
Read warning label on alcohol product before using.
If you have to use any other solution for medical reasons please contact the Global Customer Support Center for more information.

WARNING: Avoid exposing this product to contact with hot oil or other flammable liquids. If such exposure occurs, unplug the device and clean the product immediately in accordance with these guidelines.

Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, bleach/sodium hypochlorite[1] **(see important note below)**, hydrogen peroxide, ammonium chloride or mild dish soap.

- Use pre-moistened wipes and do not allow liquid cleaner to pool.

[1]When using sodium hypochlorite (bleach) based products always follow the manufacturer's recommended instructions: use gloves during application and remove the residue afterwards with a damp alcohol cloth or a cotton swab to avoid prolonged skin contact while handling the device.

Due to the powerful oxidizing nature of sodium hypochlorite the metal surfaces on the device are prone to oxidation (corrosion) when exposed to this chemical in the liquid form (including wipes). In the event that these type of disinfectants come in contact with metal on the device, prompt removal with an alcohol-dampened cloth or cotton swab after the cleaning step is critical.