

XPRESSENTRY

Secure Device Management (SDM)

By



Table of Contents

Table of Contents.....	2
Purpose.....	4
Key Features.....	4
Remote Command Execution.....	4
Security Controls.....	4
App Updates and File Sharing.....	4
Unsupported Devices.....	4
Understanding the QR Code Contents.....	4
Obtaining the QR Code.....	5
Creating a Registration Session (Server-Based QR).....	5
HTTP Pre-Requisite.....	5
Creating a Registration Session.....	8
Provisioning a Device.....	10
Accepting/Denying Devices	14
Device Approval.....	15
Legacy Device Registration.....	17
Sending Remote Commands.....	19
Kiosk Mode.....	21
Setting Kiosk Password.....	22
Installing/Updating Apps.....	24
Sending Files.....	26
Restricting Hardware (SDM Profiles).....	27
.....	29
.....	30

Purpose

This update enhances XPressEntry by introducing **Secure Device Management (SDM)** capabilities. SDM enables **centralized control of handheld devices**, allowing administrators to remotely control and manage devices, enforce security policies, and restrict unauthorized access.

In addition to SDM functionality, this update includes **improvements to the reader setup process** and **enhanced certificate handling**.

Key Features

Remote Command Execution

Administrators can send commands to managed devices, including:

- Enable Kiosk Mode (locks the device to the XPressEntry application)
- Disable Kiosk Mode (via remote command or password entry on the device)
- Reset XPressEntry application data
- Perform a full factory reset

Security Controls

- Enable or disable hardware features (USB, SD card, SIM, etc.)
- Apply device restrictions using SDM profiles

App Updates and File Sharing

- Remotely install or update applications (APK files)
- Send files directly to devices.

Unsupported Devices

Devices running unsupported versions earlier than **3.7.28 (excluding 3.7.21-DPC)** will appear as unsupported and will not be able to receive remote commands until the app is updated. All other device functionalities will remain available.

Understanding the QR Code Contents

Provisioning QR codes are used to configure devices for **Android Enterprise enrollment**. Each QR code contains an encoded JSON payload with configuration details required for provisioning.

The QR Code includes:

- Download locations for XPressEntry and KeyLink APKs

- Package checksums for validation
- Wi-Fi configuration (if applicable)
- Certificate and encryption settings

Obtaining the QR Code

There are two primary ways for obtaining a provisioning QR code:

1. **XPressEntry Server** (Recommended)
 - Automatically connects devices to the configured server
 - Includes server and Wi-Fi configuration
 - Supports registration sessions and approval workflows
2. telaeris.com/downloads
 - Installs the application only
 - Requires manual configuration after installation
 - Does not include server or Wi-Fi information

Creating a Registration Session (Server-Based QR)

A **Registration Session** defines a **controlled time window** during which devices can register with the XPressEntry Server. When creating a session, users can configure:

- Session name and description
- Expiration time
- Maximum number of devices
- Server connection details
- Wi-Fi configuration (optional)
- APK download locations

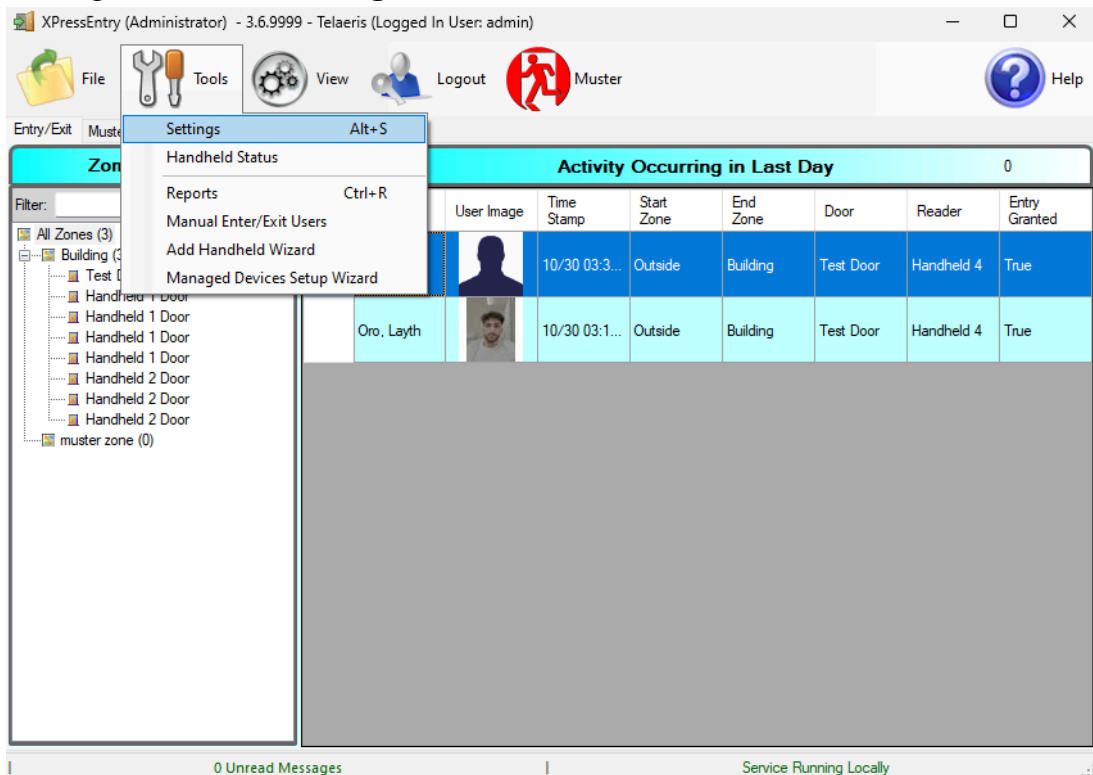
Note: Devices scan the session's QR code and enter a **pending state** until approved by an administrator. If the **auto-approve device option** is enabled for the session, devices are approved immediately and do not enter a pending state.

HTTP Pre-Requisite

If the XPressEntry server uses a **self-signed certificate**, HTTP must be enabled for initial device provisioning. Android requires certificates signed by a trusted authority. If the certificate is not trusted, HTTPS connections will fail during initial setup. HTTP allows the device to download the application before switching to secure HTTPS communication. Once the APK is downloaded and installed, all other requests will be performed securely over HTTPS, unless the customer has configured the server to only use HTTP in the server settings.

When provisioning a device from a factory reset, an **active internet connection is required**. On-premises customers on a local network should temporarily connect to a Wi-Fi network with internet access, scan the QR code from telaeris.com/downloads, and then switch back to their on-premises network to connect to their XPressEntry server.

1. Navigate to **Tools > Settings > Server**



1. Enable **HTTP w/ SSL**
2. Ensure the selected port (**default: 30000**) is open in the firewall

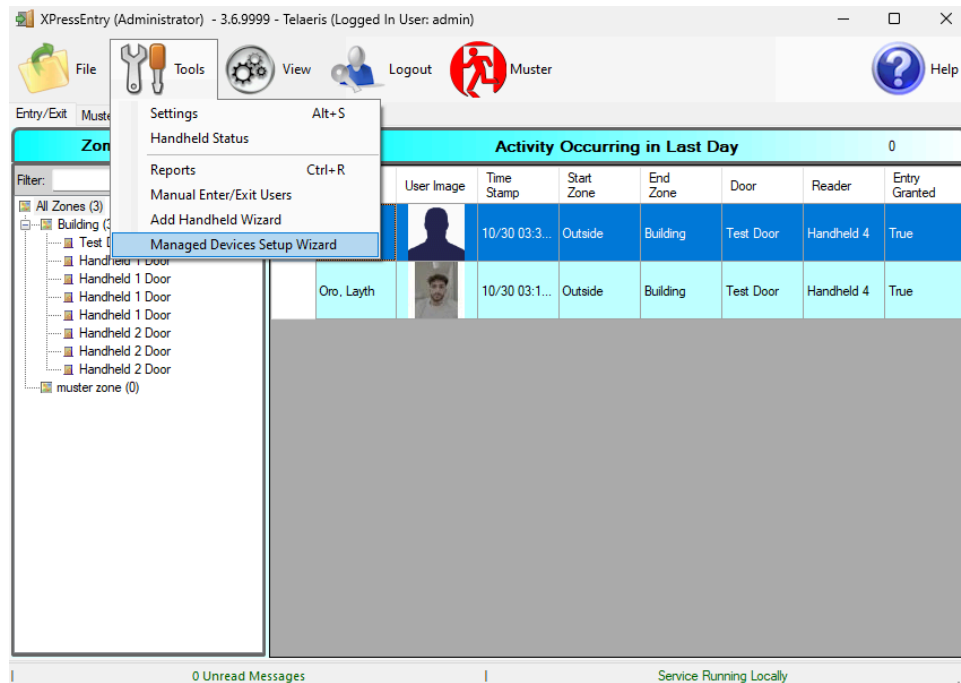
XPressEntry Settings
File Database SQL Import/Export

General
Add / Edit Display
Badges
RFID
User Defined Fields
Muster Settings
Question Setup
Logging
Client Settings
Wiegand Format Data
LDAP Settings
Server
Service Settings
Database
Data Manager
Software Event Viewer
Reader Profiles
Handheld Functionality
Reader Validations
Passwords
Badge Settings
Custom Display
Validation Colors
Doors
Trend Settings
Panic Alarm Settings
Location And Battery
Alarm Settings
Alarm Targets
Email Settings
Twilio Settings
Copy Resx File

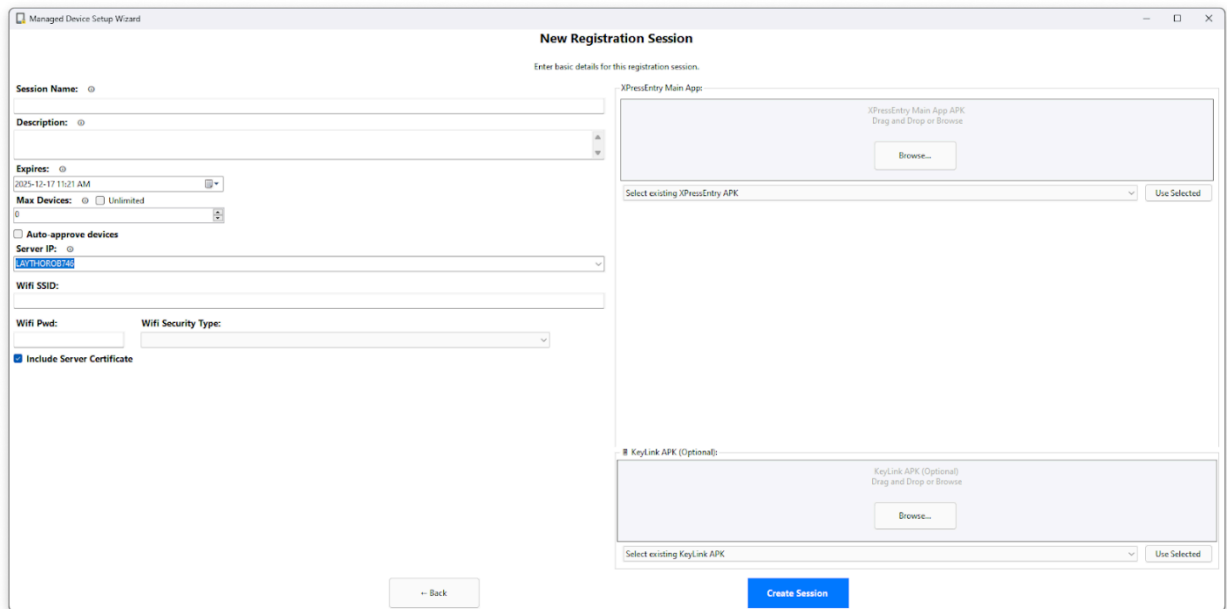
XPressEntry Service
Service: Stopped
Service Type: Local Windows Service
Service Host Name: localhost
Certificate Identity: XPressEntryService
Validate Service Certificate: ☐
Service Certificate
HTTP/S Handheld Server
☒ HTTP w/ SSL HTTP Port: 30000 ☐ Use Legacy HTTP Server
☒ Enable HTTPS SSL Port: 30001 Certificate
☒ SSL Websocket
Push Interval(ms): 5000
SSL Thumbprint: BDD5AF912E2E9284143911810349FE1CDE083D9C
SSL Cert Info:
Subject: CN=XPressEntryService
Issuer: CN=XPressEntryService
Thumbprint: ABE52172A199CC2595E6E2E828A68A2EE1F879A
2
Name/IP for Clients: 10.10.8.131
Let's Encrypt Certificate
Server Domain:
Admin Email:
Renewal Interval(days): 0
Check and Get Certificate Now
Clear Let's Encrypt Account Settings
Result:
Save Cancel

Creating a Registration Session

1. Navigate to **Tools > Managed Devices Setup Wizard**



2. Enter the following details:
 1. Session name and description
 2. Expiration and device limit
 3. Server IP address
 4. Wi-Fi settings (optional)
 5. XPressEntry APK
 6. Optional KeyLink APK



Managed Device Setup Wizard

New Registration Session

Enter basic details for this registration session.

Session Name:

Description:

Expires:

Max Devices: ☐ Unlimited

☐ Auto approve devices

Server IP:

Wifi SSID:

Wifi Pwd: **Wifi Security Type:**

☒ Include Server Certificate

XPressEntry Main App:

XPressEntry Main App APK
Drag and Drop or Browse

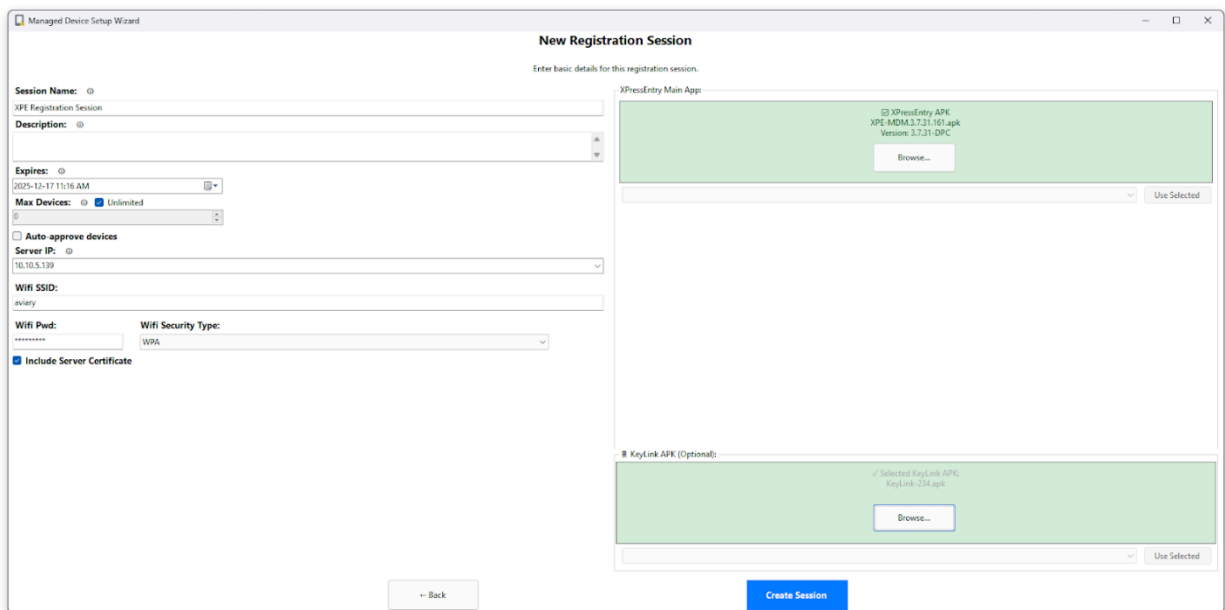
Select existing XPressEntry APK

KeyLink APK (Optional):

KeyLink APK (Optional)
Drag and Drop or Browse

Select existing KeyLink APK

3. Click Create Session



Managed Device Setup Wizard

New Registration Session

Enter basic details for this registration session.

Session Name:

Description:

Expires:

Max Devices: ☒ Unlimited

☐ Auto approve devices

Server IP:

Wifi SSID:

Wifi Pwd: **Wifi Security Type:**

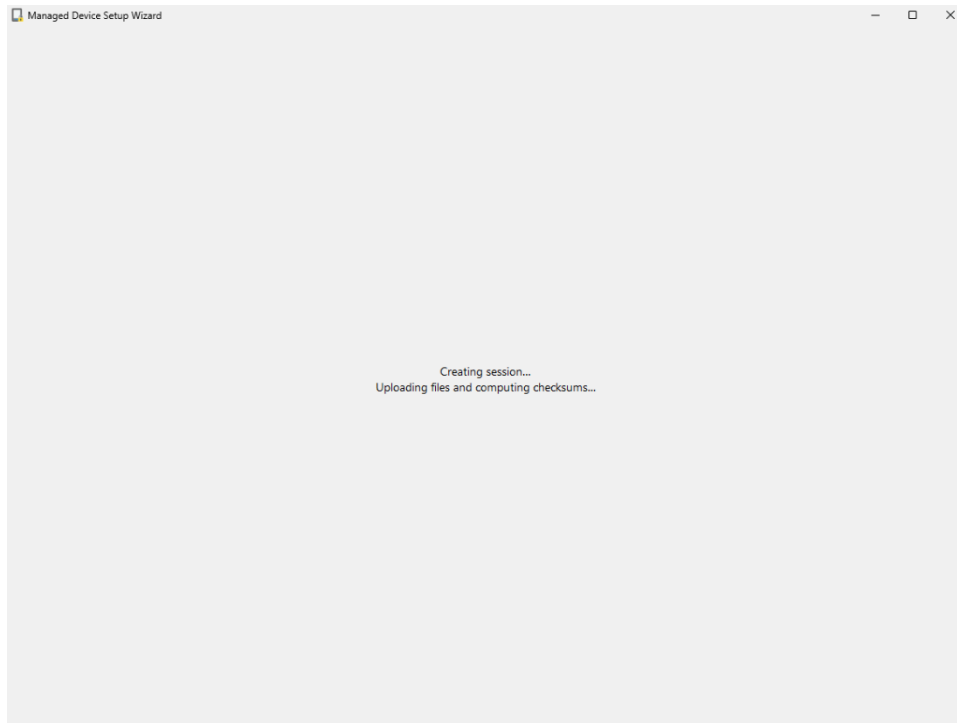
☒ Include Server Certificate

XPressEntry Main App:

XPressEntry Main App
XPE.MDM3.7.31.161.apk
Version: 3.7.31-DPC

KeyLink APK (Optional):

✓ Selected KeyLink APK:
KeyLink-234.apk



4. The manage registration session page will open. Users can select the session created and view the QR code, as well as modify the session information if needed.
5. This QR code can be used to register **regular, SDM, and factory-reset devices**:
 1. **Regular devices**
 1. When scanned within the XPressEntry app, the device opens the *Awaiting Approval* page (if auto-approval is disabled)
 2. An administrator must approve the device before it can connect to the server.
 2. **SDM builds**
 1. These follow the same approval process as regular devices
 2. Can automatically connect to Wi-Fi using credentials embedded in the QR code and update the app to the specified version if a newer version is available
 3. **Factory-reset devices**
 1. When scanned from the device's welcome screen, the QR code provisions the device for SDM and installs XPressEntry (and KeyLink, if included)
 2. Places the device in a **pending state** until approved by an administrator

Provisioning a Device

Before a device can be provisioned for SDM mode, it must be **factory reset**. A factory-reset device will look like the example shown below.

Hi there

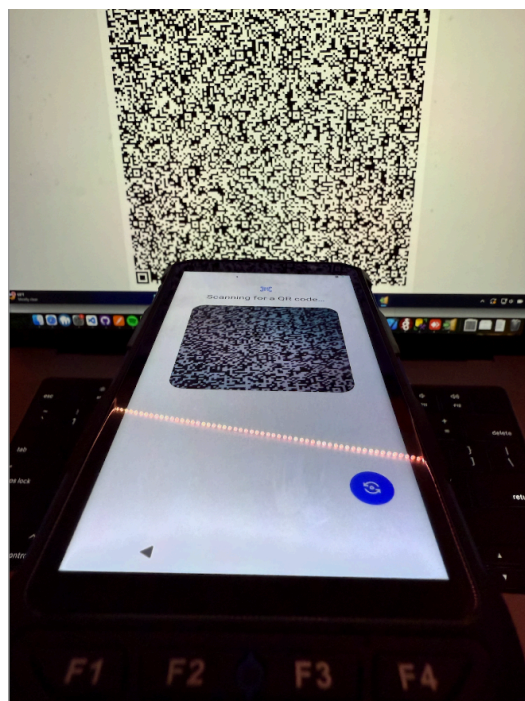
🌐 English (United States)

👁 Vision settings

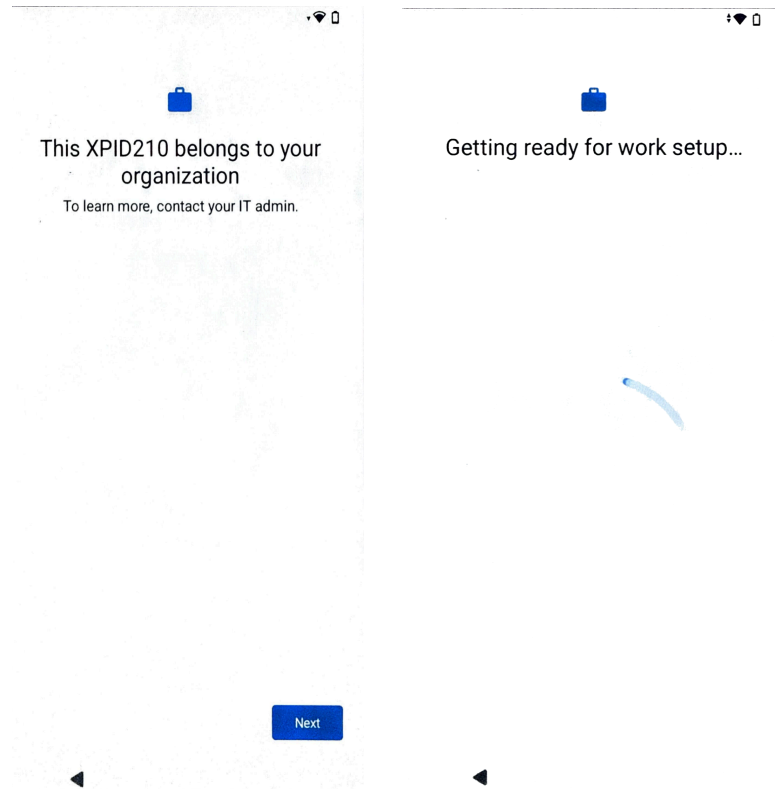
Emergency call

Start

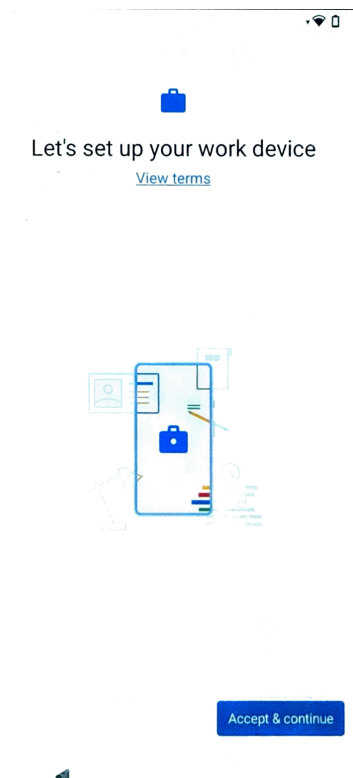
1. On a factory-reset device, tap anywhere on the welcome screen **six times in a row**.
2. Scan the provisioning QR code



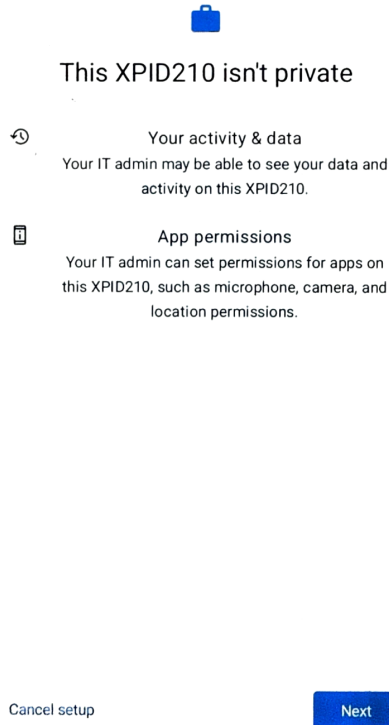
3. Select **Next**.



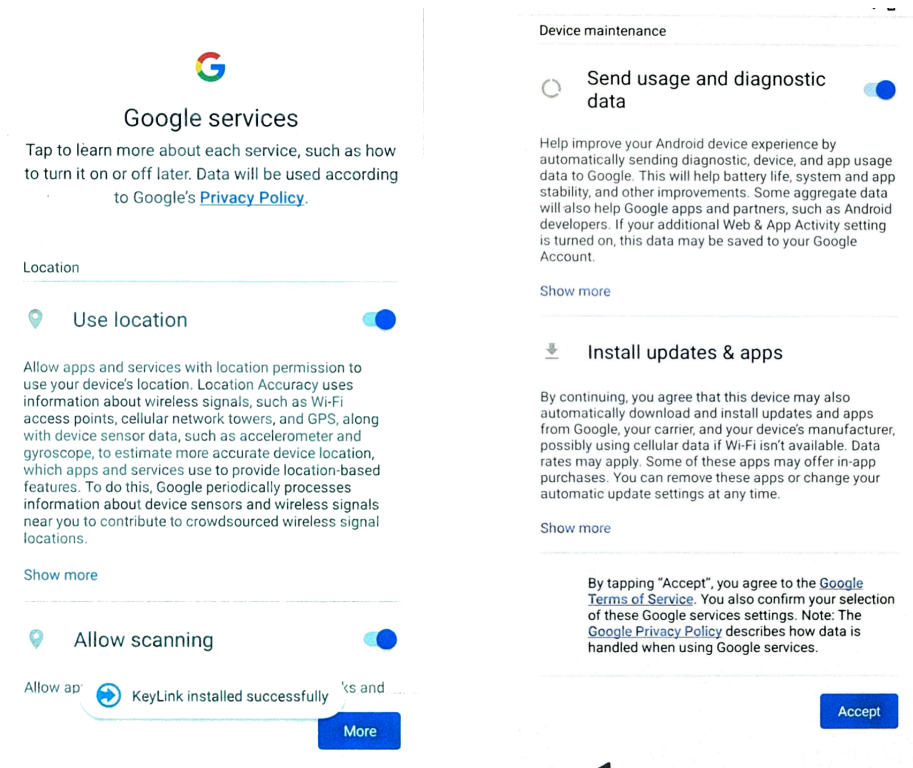
4. Then, select **Accept & Continue**.



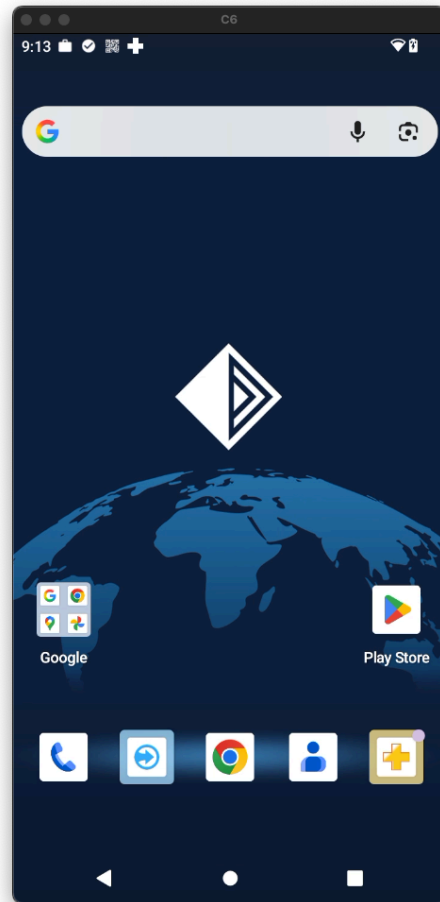
5. Select **Next**.



6. Select **More**, then **Accept**.



7. After clicking Accept, you are redirected to the home screen. KeyLink will be installed if a KeyLink APK was selected during session creation.



Accepting/Denying Devices

If the QR code generated by the XPressEntry server is scanned, the device will appear in a **Pending state** on the Manage Devices page. The device must be approved by an administrator before it can connect to the server.

Once the QR code from telaeris.com/downloads is scanned, the XPressEntry application will launch in its **default demo mode** and will not be connected to a server.

To complete setup using the website QR code:

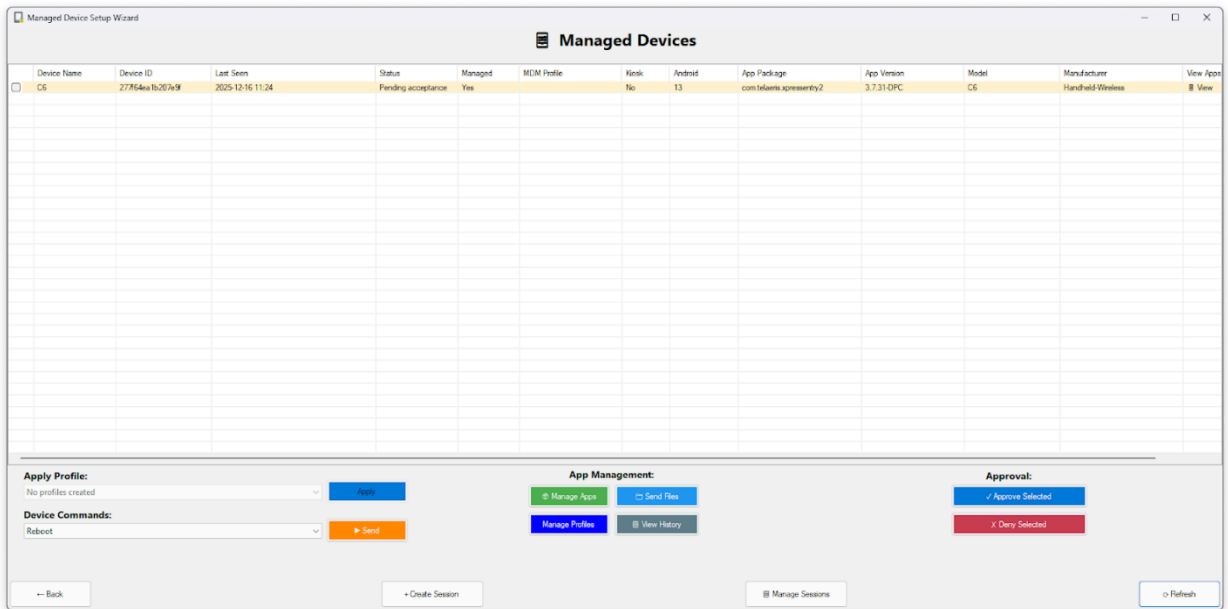
1. Create a **Registration Session** in XPressEntry
2. Navigate to the **Reader Setup page**
3. Select **Quick Setup QR Code**
4. Scan the Registration Session QR code

After scanning, the application will:

- Attempt to connect to the configured Wi-Fi network (if included)
- Save certificate information (if provided)
- Update the application to the version specified in the QR code, if a newer version is available

Device Approval

1. Navigate to the **Manage Devices** page to review pending devices.
2. To Approve Devices:
 - a. Select the checkbox next to the desired device(s)
 - b. Click the blue **Approve Selected** button in the bottom-right corner of the screen



The screenshot shows the 'Managed Device Setup Wizard' window with a 'Managed Devices' section. It contains a table with columns: Device Name, Device ID, Last Seen, Status, Managed, MDM Profile, Kiosk, Android, App Package, App Version, Model, Manufacturer, and View Apps. The first row shows a device named 'C6' with ID '27764aa1b207a9f', last seen on '2025-12-16 11:24', status 'Pending acceptance', and managed 'Yes'. Below the table are three main sections: 'Apply Profile' with a dropdown and an 'Apply' button; 'Device Commands' with a dropdown and a 'Send' button; 'App Management' with buttons for 'Manage Apps', 'Send Files', 'Manage Profile', and 'View History'; and 'Approval' with 'Approve Selected' and 'Deny Selected' buttons. At the bottom are buttons for 'Back', 'Create Session', 'Manage Sessions', and 'Refresh'.

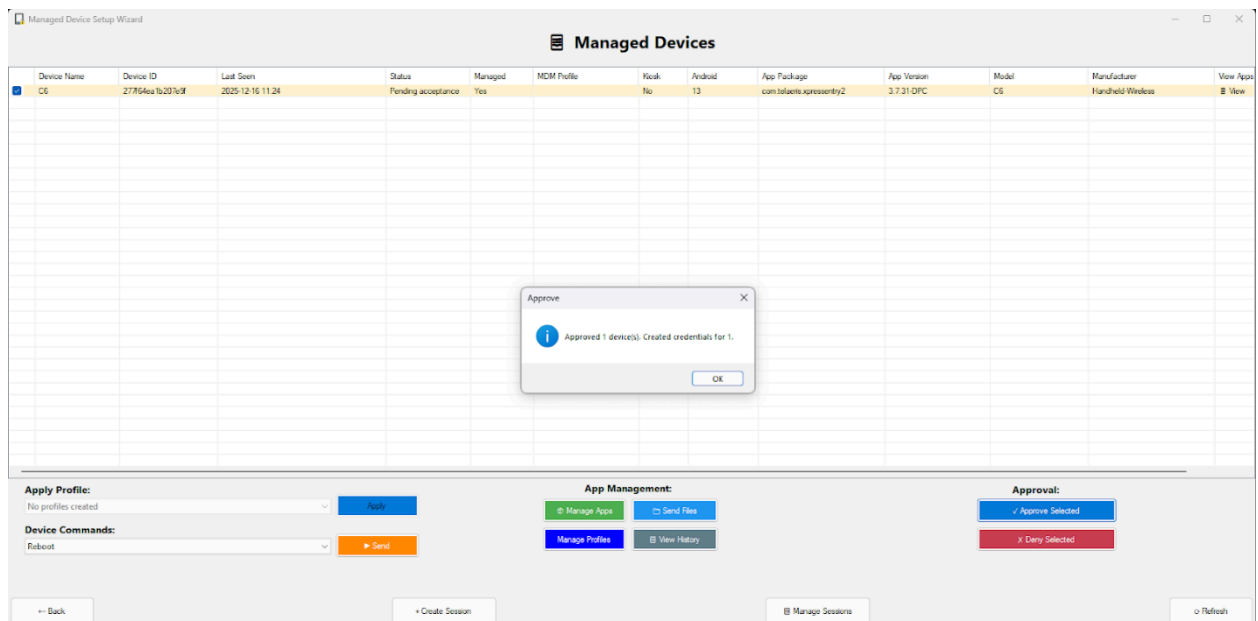
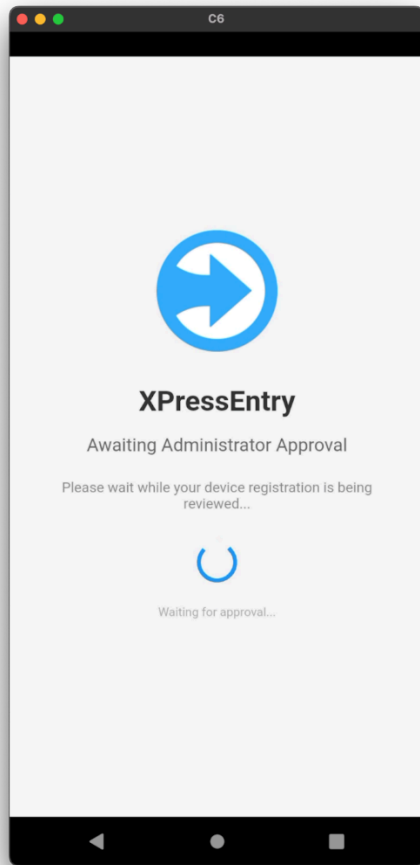
Device Name	Device ID	Last Seen	Status	Managed	MDM Profile	Kiosk	Android	App Package	App Version	Model	Manufacturer	View Apps
C6	27764aa1b207a9f	2025-12-16 11:24	Pending acceptance	Yes		No	13	com.telaeris.apressentry2	3.7.31-DPC	C6	Handheld Wireless	View

Apply Profile:
 No profiles created
 Device Commands: Reboot
 Apply Send

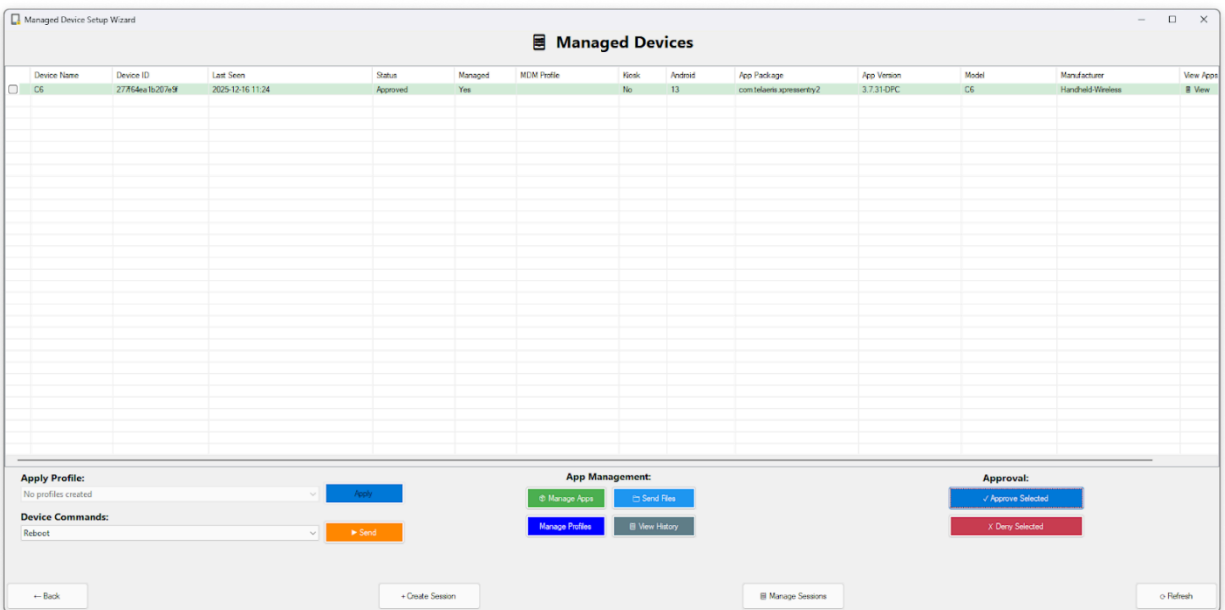
App Management:
 Manage Apps Send Files
 Manage Profile View History

Approval:
 Approve Selected
 Deny Selected

Back Create Session Manage Sessions Refresh

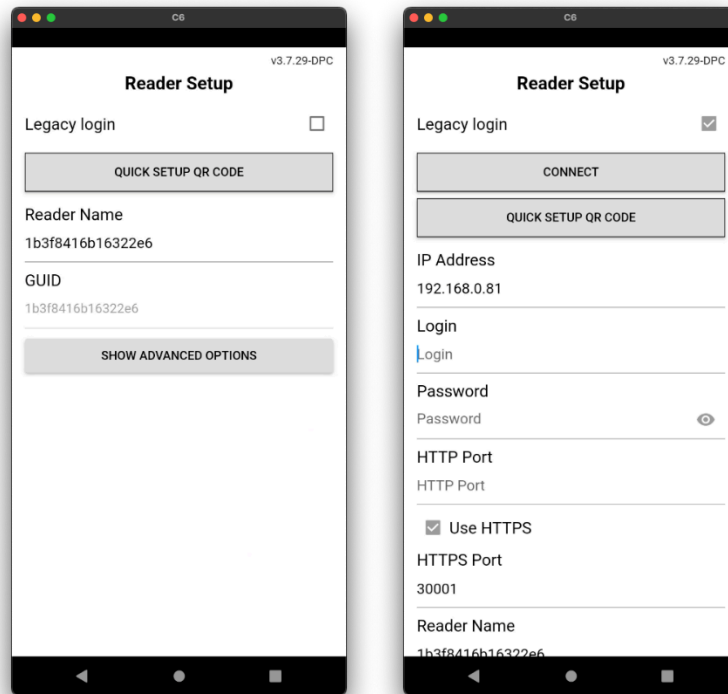


3. The device should now change from **yellow (pending)** to **green (approved)** and receive a credential
4. Once the device is approved, the application will launch automatically if needed and complete synchronization

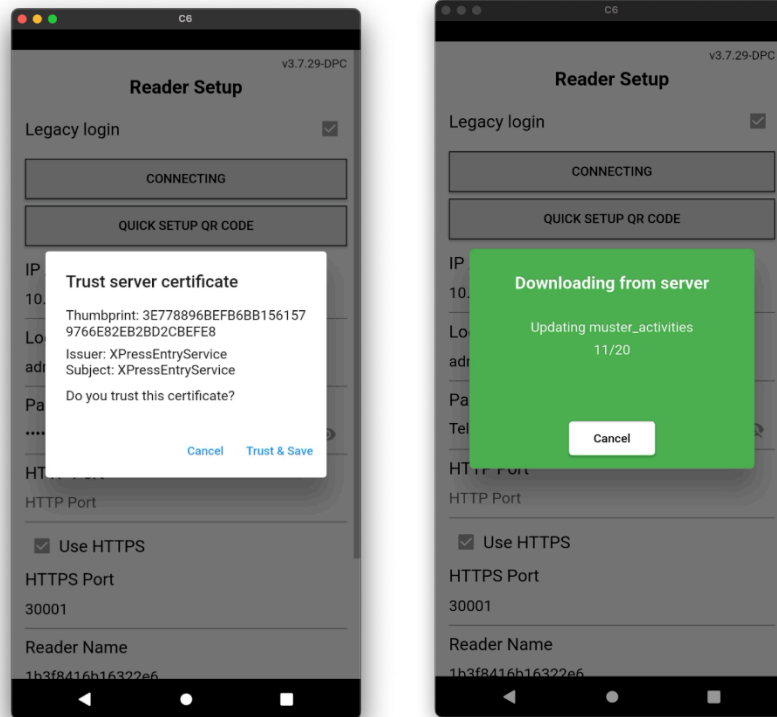


Legacy Device Registration

All devices can continue to be registered using a QR code. The traditional username and password login method is now available through the **Legacy Login** button on the Reader Setup page. Selecting this option will display the legacy connection details, including IP address, username, password, and related settings.



When connecting to an XPressEntry server that uses a **self-signed certificate**, you will be prompted to trust and save the certificate. Saving the certificate allows the system to detect any future changes. If the certificate changes, you will be notified and given the option to review and decide whether to trust the new certificate.



Sending Remote Commands

To send remote commands (such as entering kiosk mode), select the target devices, then click the orange **Send** button.

Available commands currently include **reboot**, **enter or exit kiosk mode**, **enable or disable USB**, **SD card**, and **SIM access**, **reset data**, and **wipe the device**.

Managed Device Setup Wizard

Managed Devices

Device Name	Device ID	Last Seen	Status	Managed	MDM Profile	Kiosk	Android	App Package	App Version	Model	Manufacturer	View Apps
C6	27f54dea1b207a9f	2025-12-16 11:24	Approved	Yes		No	13	com.telaeris.xpressentry2	3.7.31-OPC	C6	Handheld-Wireless	View

Apply Profile:

No profiles created

Test

Device Commands:

Enter Kiosk

Reboot

Enter Lock

Exit Kiosk

Reset Data

Wipe

Send

App Management:

Manage Apps

Send Files

Manage Profiles

View History

Approval:

Approve Selected

Deny Selected

Create Session

Manage Sessions

Refresh

You can view the status of sent commands by clicking the gray **View History** button. Commands that have been sent but have not yet returned a response are shown **in cyan**. Successfully executed commands appear **in green** with a result status, while failed commands are displayed **in red**.

Managed Device Setup Wizard

MDM Command History

3 commands found

Command ID	Reader ID	Device Name	Command Type	Parameters	Status	Result Status	Sent By	Date/Time	Acknowledged At
1837	2240	C6	enter_kiosk		sent		Company Adminstr...	2025-11-12 02:51:17	
1836	2240	C6	exit_kiosk		completed	success	Company Adminstr...	2025-11-12 02:03:33	2025-11-12 10:03:33
1835	2240	C6	enter_kiosk		completed	success	Company Adminstr...	2025-11-12 02:03:06	2025-11-12 10:03:06

Back

Previous

Next

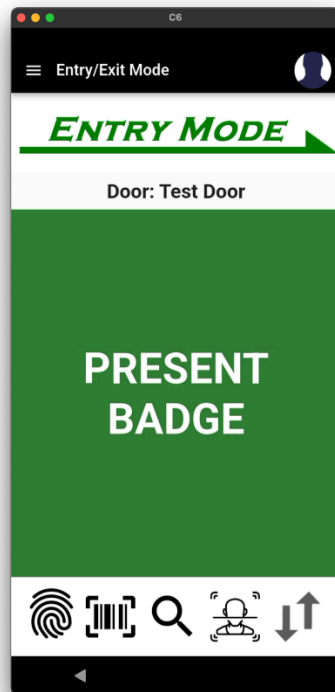
Refresh

Page 1 of 1

Kiosk Mode

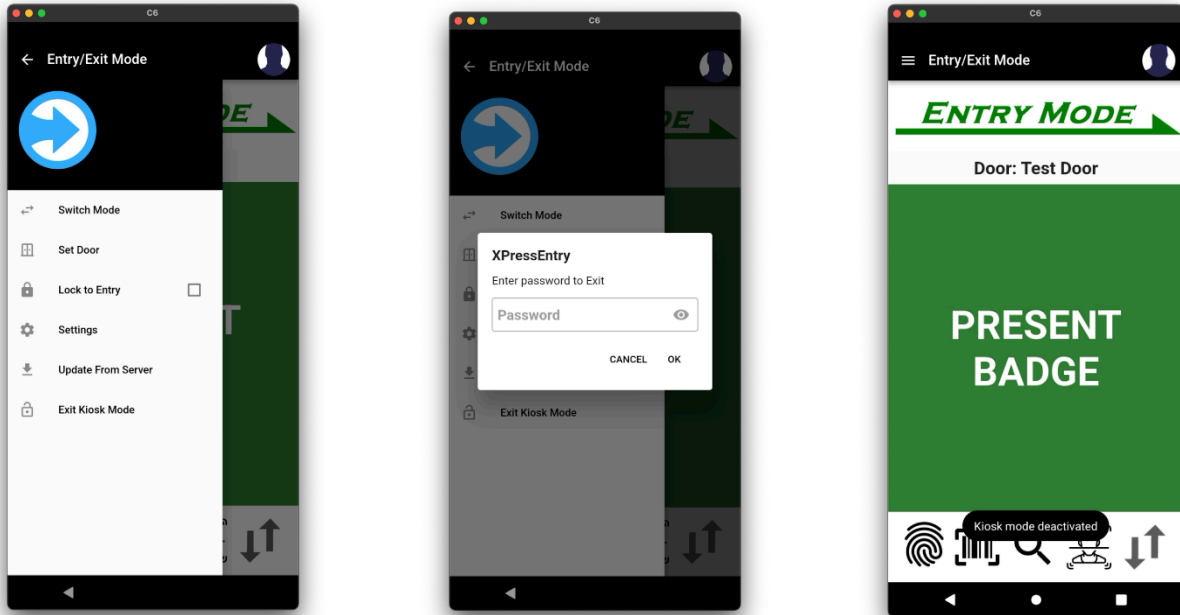
Kiosk Mode locks the device to the XPressEntry app and prevents access to all other functions.

When the **Enter Kiosk** command is sent, the device is forced into the XPressEntry app, even if it is asleep or the app is not currently in the foreground. While in Kiosk Mode, only the **back arrow** is available, and users cannot exit the app or access service settings.



To exit Kiosk Mode, either send the **Exit Kiosk** command or enter the preset password within the app.

The Exit Kiosk option is located in the app's main drawer. After the correct password is entered, Kiosk Mode will end, the server will be notified, and the app can be exited normally.



Setting Kiosk Password

Setting a password to exit Kiosk Mode is recommended to ensure **secure access control**.

If an **Enter Kiosk** command is sent without a password configured, a dialog will appear with the following options:

- **Send Anyway**
 - Clicking Send Anyway will still send the command to the device; however, the device will not be able to exit Kiosk Mode manually. In this case, an Exit Kiosk command must be sent for the device to leave Kiosk Mode.
- **Settings**
 - Clicking Settings opens the reader profile's password page, where a password can be configured for exiting Kiosk Mode from within the app.
- **Cancel** - Cancel the action

Note: Sending the command without a password will allow users to exit Kiosk Mode **without authentication**.

Managed Device Setup Wizard

Managed Devices

Device Name	Device ID	Last Seen	Status	Managed	MDM Profile	Kiosk	Android	App Package	App Version	Model	Manufacturer	View Apps
C6	27f54ea1b207c9f	2025-12-16 11:24	Approved	Yes		No	13	com.telaeris.xpressentry2	3.7.31-DPC	C6	Handheld-Wireless	View

Enter Kiosk Warning

No exit password is configured.
Without a password, the device can only exit kiosk mode via remote command.
What would you like to do?

Apply Profile:

No profiles created

Device Commands:

Enter Kiosk

App Management:

Approval:

Managed Device Setup Wizard

Managed Devices

XPressEntry Settings

File Database SQL Import/Export

- General
 - Add / Edit Display
 - Badges
 - RFID
 - User Defined Fields
 - Muster Settings
 - Question Setup
 - Logging
 - Client Settings
 - Wiegand Format Data
 - LDAP Settings
- Server
 - Service Settings
 - Database
- Data Manager
 - Software Event Viewer
- Reader Profiles
 - Handheld Functionality
 - Reader Validations
 - Passwords
 - Badge Settings
 - Custom Display
 - Validation Colors
 - Doors
 - Trend Settings
 - Panic Alarm Settings
 - Location And Battery
 - Musters
 - Biometric Settings
- Alarm Settings
 - Alarm Targets
 - Email Settings
 - Twilio Settings
 - Copy Resx File

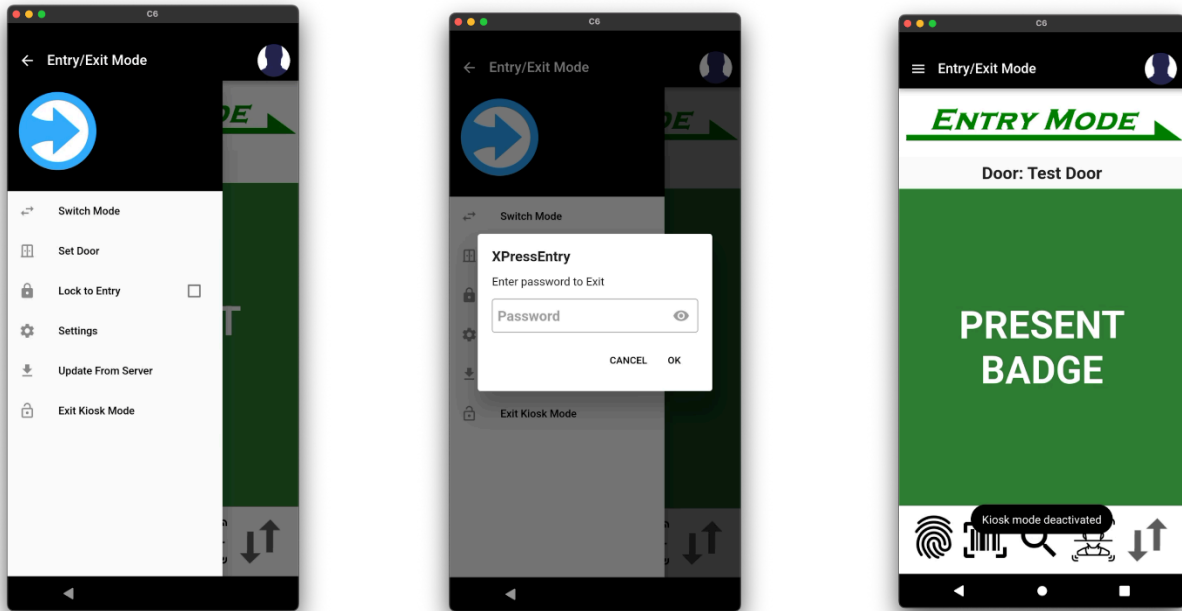
Profiles

Default Selected: Default

Main Setup Password: **** ☐ Show Passwords

If you do not set a password for an individual mode but have a setup password set then the setup password will be used by default

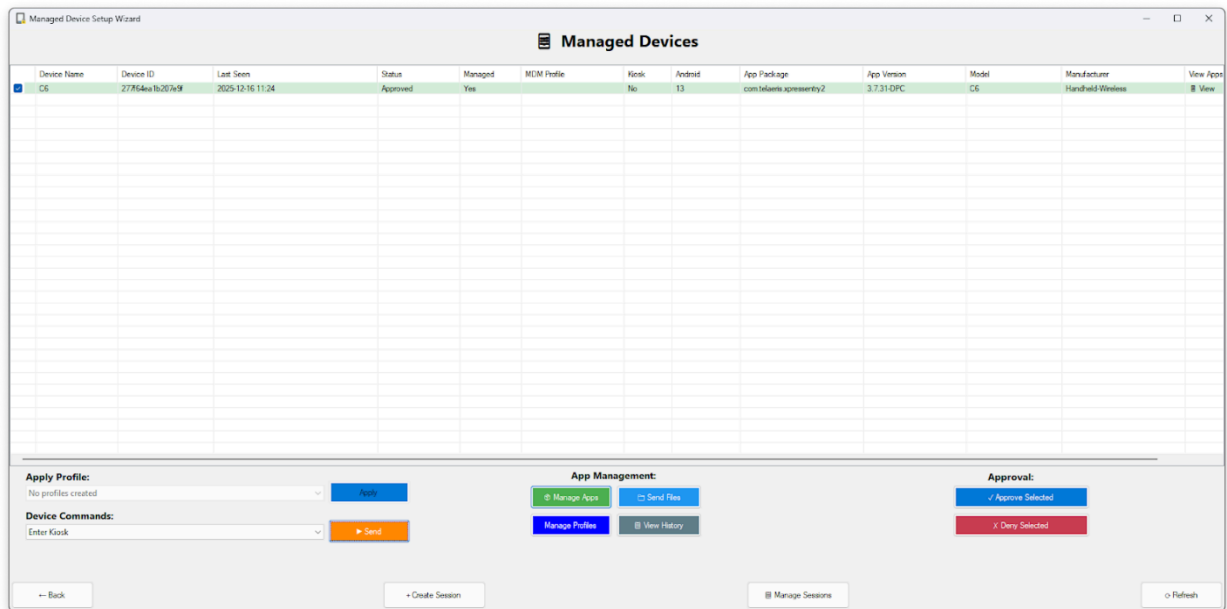
- ☐ Password for Set Door
- ☐ Password for Lock Mode
- ☐ Password for Occupancy
- ☐ Password for Activity
- ☐ Password for Entry/Exit
- ☐ Password for Muster
- ☐ Password for Verification
- ☐ Password to Set Zone
- ☐ Password for Enroll
- ☐ Password for Freedom
- ☐ Password for Search Users
- ☐ Password for Settings
- ☒ Password for Exiting App
- ☐ Password for Lockscreen



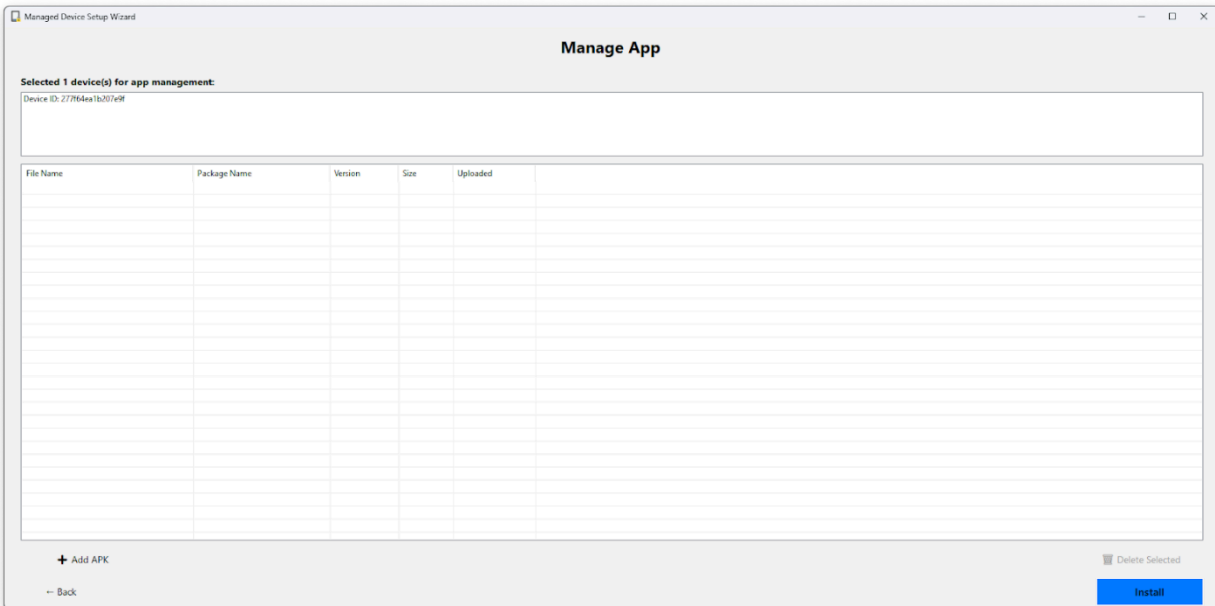
Installing/Updating Apps

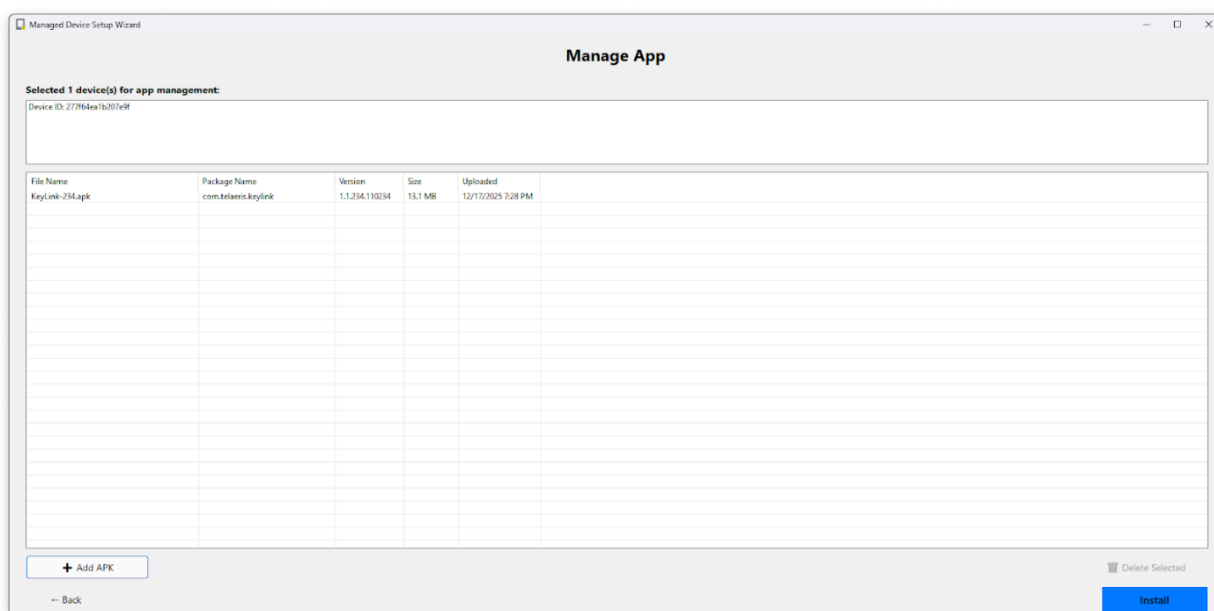
To install or update applications:

1. Click the green **Manage Apps** button.



2. Select the APK you want to install or update, then click **Install**.



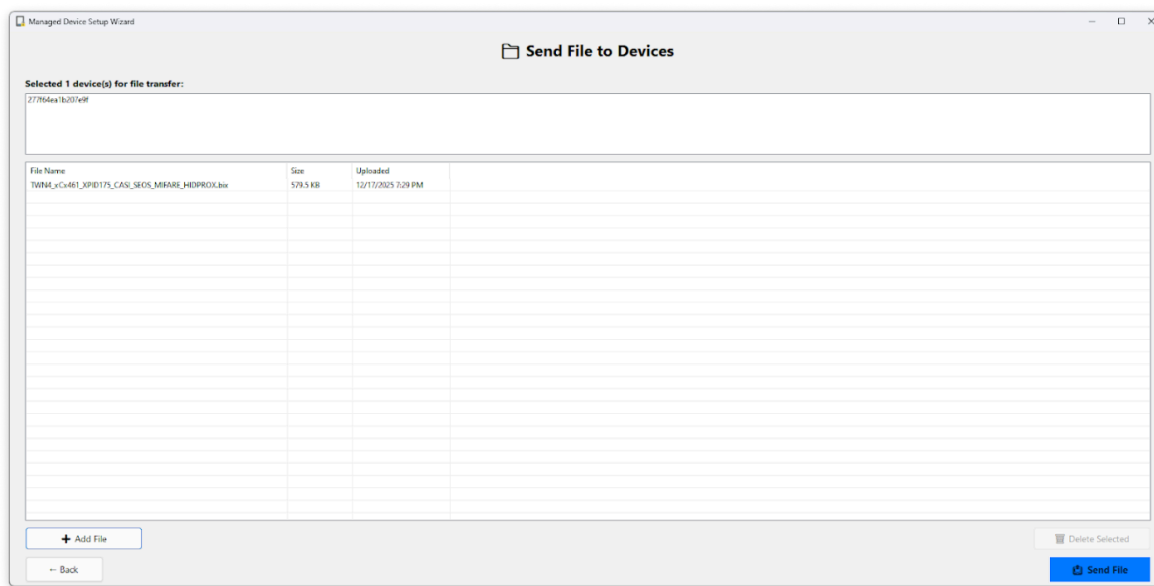


Sending Files

To send files to devices:

1. Select the target devices
2. Click the blue **Send File** button

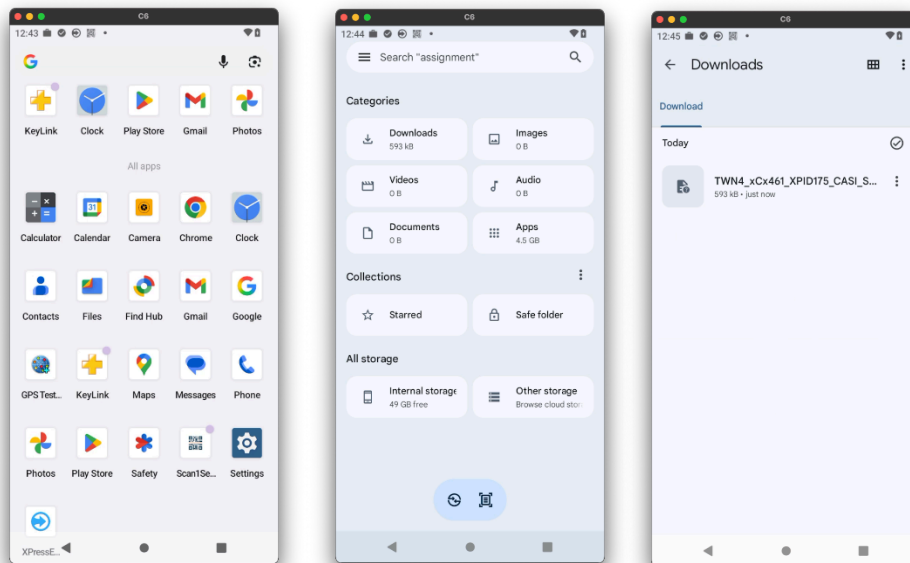
Note: The selected file will be sent to the **Downloads** directory on each of the chosen devices.



Restricting Hardware (SDM Profiles)

Devices configured in SDM mode can be managed using **SDM profiles**, which allow administrators to restrict various device capabilities. Examples include, but are not limited to:

- Enabling or disabling the camera
- SIM access
- USB access



To create an MDM profile, select the **Manage Profiles** button.

Managed Device Setup Wizard

Create New MDM Profile

General

Profile Name:

Connectivity

☒ Enable SIM

☒ Auto Reconnect WiR

Add

Edit

Remove

Hardware Restrictions

☒ Enable USB

☒ Enable SD Card

☒ Enable Bluetooth

☒ Enable Camera

☒ Enable GPS

← Back

Save

Managed Device Setup Wizard

Create New MDM Profile

General

Profile Name:

Connectivity

☒ Enable SIM ☒ Auto Reconnect WiFi

SSID:

Password:

Security:

☐ Use as Locked Network

Add

Edit

Remove

Hardware Restrictions

☒ Enable USB ☒ Enable SD Card ☒ Enable Bluetooth

☒ Enable Camera ☒ Enable GPS

Managed Device Setup Wizard

MDM Profiles

XPE Profile

USB SIM SD Card WiFi

Bluetooth Camera GPS

Managed Device Setup Wizard

Managed Devices

Device Name	Device ID	Last Seen	Status	Managed	MDM Profile	Risk	Android	App Package	App Version	Model	Manufacturer	View App
CS	277654ea7b207e9f	2025-12-16 11:24	Approved	Yes		No	13	com.telaris.xpresentry2	3.7.31-OPC	CS	Handheld-Wireless	View App

Apply Profile:

XPE Profile

Apply

Device Commands:

Reboot

Send

App Management:

Manage Apps

Send Files

Manage Profiles

View History

Approval:

Approve Selected

Deny Selected

Back

Create Session

Manage Sessions

Refresh

Managed Device Setup Wizard

Managed Devices

Device Name	Device ID	Last Seen	Status	Managed	MDM Profile	Risk	Android	App Package	App Version	Model	Manufacturer	View App
CS	277654ea7b207e9f	2025-12-16 11:24	Approved	Yes		No	13	com.telaris.xpresentry2	3.7.31-OPC	CS	Handheld-Wireless	View App

Confirm Apply

Apply profile 'XPE Profile' to 1 device(s)?

Yes

No

Apply Profile:

XPE Profile

Apply

Device Commands:

Reboot

Send

App Management:

Manage Apps

Send Files

Manage Profiles

View History

Approval:

Approve Selected

Deny Selected

Back

Create Session

Manage Sessions

Refresh

[illegible]