Veilora Secure Terminal Guide

Contents

0. Introduction 4

0.1 About This Manual 4

0.2 Safety and Compliance Statement 4

1. Quick Start 6

1.1 Getting to Know Your Device 6

1.2 Initial Setup Guide 7

1.3 System Account Management 10

1.4 Quick App Installation 15

2. How to Create and Set Up a Private Space 16

2.1 System-Wide Multi-Level Isolated Encrypted Storage 16

2.2 Initializing Private Space 16

2.3 Setting Up "Dual PINs" for Space Switching 17

2.4 Cross-Space File Synchronization Guide (Main Space ➔ Private Space) 19

3. How to Reduce the Risk of Online Profiling 22

3.1 Anti-Tracking Profiling and Proactive Network Attack Protection 22

3.2 Intelligent Abnormal Traffic Control 22

4. How to Prevent App Privacy Theft 24

4.1 App Permission Control and Risk Auditing 24

4.2 One-Tap Super Privacy Mode 25

5. How to Reduce the Risk of Data Leakage Through Third-Party Retention in Instant Messaging 27

5.1 Enabling the Encrypted Conversion Tool 27

5.2How to Send Encrypted Messages 29

5.3How to Send Encrypted Files 30

5.4 Viewing and Browsing Encrypted Files 36

5.5 How to Make Encrypted Voice Calls 38

6. How to Use the Private Cloud for Encrypted Backups and Restoration 40

6.1 WebDAV Cloud Space Configuration 40

6.2 Setting Up Automatic/Manual Backup Schedules 42

6.3 Local Data Recovery Process 44

7. How to Reinforce System Security 47

8. How to Perform an Emergency Reset 51

8.1 How to Reset the Entire Device 51

8.2 How to Reset the Private Space 52

8.3 How to Remotely Lock and Reset 56

0. Introduction

Thank you for choosing the VEILORA secure smartphone. In today's highly digital world, threats such as data breaches, network eavesdropping, and privacy tracking are omnipresent. VEILORA is not just an ordinary smart device; it is a "mobile digital fortress" meticulously crafted for you.

VEILORA is a professional operating system dedicated to digital privacy protection and cybersecurity. It is designed for military personnel, law enforcement officers, government officials, high-value business professionals, scientists, and other individuals who require an exceptionally high level of digital security protection. Powered by a proprietary security architecture, VEILORA integrates eight core capabilities: cybersecurity, protection, privacy management, isolated storage, encrypted communications, emergency protection, anti-extraction safeguards, secure cloud backup, and intelligent threat detection. Together, these capabilities establish a comprehensive security framework that protects data throughout its entire lifecycle—from collection and transmission to storage and use—helping safeguard endpoint devices and sensitive information at the system level.

0.1 About This Manual

This manual is designed to help you quickly understand and master the exclusive security features and daily operational guidelines of your VEILORA smartphone. Because this device incorporates unique low-level encryption and isolation mechanisms, we strongly recommend that you carefully read all sections of this manual before your first use, even if you are highly familiar with standard smartphones.

0.2 Safety and Compliance Statement

Before enjoying the ultimate secure experience brought by VEILORA, please carefully read and acknowledge the following statements and compliance terms:

1. Disclaimer: Your core security keys (such as the account recovery phrase, Private Space password, and device reset password) are exclusively stored locally in the device's hardware security module and must be kept offline by you. Our official servers absolutely do not back up or store any of your decryption credentials. If you

lose your recovery phrase or forget your password, resulting in the inability to decrypt data or a permanent device lockout, VEILORA and its authorized service providers cannot offer forced unlocking or data recovery services, nor will we bear any joint liability for any direct or indirect data loss arising from such situations.

2. Security Usage Responsibilities: The advanced security features provided by this device, such as Encrypted Instant Messaging, One-Tap Recovery, and Network Stealth, are designed to protect users' lawful communication privacy and legitimate digital assets. As the sole owner of the device, you must properly safeguard the device and its security credentials, and assume all legal consequences arising from its use. It is strictly prohibited to use this device for any illegal activities that violate the laws and regulations of your local country or region.

3. System Integrity Statement: Do not attempt any unauthorized privilege escalation (Rooting), bootloader unlocking, or flashing of third-party firmware on this device. Such high-risk operations will trigger an irreversible device lockout or complete data wipe, and will immediately void your warranty.

1. Quick Start

Welcome to your VEILORA secure smartphone. Upon powering on for the first time, the built-in exclusive secure setup assistant will guide you through the basic configuration and establish a unique, trusted binding between the device and your personal account. Please ensure a stable network connection and carefully follow the steps below to complete the setup.

1.1 Getting to Know Your Device

This section provides a hardware overview of the device (based on the Pixel 9 Pro XL architecture), including physical button functions, interface specifications, and usage precautions, to help you quickly familiarize yourself with the hardware.



① Power Button (Side Button):

Normal operation: Press to wake or lock the screen; press and hold to bring up the power off or restart menu.

② Volume Buttons: Used to adjust the volume for calls, media, and system notifications. Press the Power Button and Volume Down Button simultaneously to take a screenshot.

③ Front Camera: Used for daily photography and encrypted video calls.

④ Rear Camera System: Includes an ultra-high-resolution main camera, an ultra-wide-angle lens, and a telephoto lens. Used for everyday recording or scanning private QR codes for secure account binding.

⑤ SIM Card Tray: Located on the bottom edge of the device. Use the ejector tool to pop out the tray and insert your physical SIM card.

⑥ USB-C Port:

Normal operation: Supports high-speed fast charging and data transfer.

⑦ Microphone Array: Distributed at the top and bottom of the device for clear audio pickup and encrypted voice calls. Similar to the camera, an exclusive green warning indicator will appear in the top right corner of the screen when the microphone is accessed.

⑧ Stereo Speakers: Comprising the top earpiece and bottom speaker, delivering high-quality audio for voice calls and media playback.

1.2 Initial Setup Guide

① Welcome Screen

As shown in Figure 1-1, this is the first screen after powering on. Here, you can select your system language (e.g., English) or configure accessibility options as needed. Once confirmed, tap Next in the bottom right corner to officially begin the configuration process.

② Connecting to a Wi-Fi Network

As shown in Figure 1-2, to ensure the smooth completion of subsequent account registration and hardware fingerprint verification, toggle on the Wi-Fi switch and connect to a trusted wireless network. Once connected successfully, tap Next to continue.

③ Logging into your VEILORA OS Account

As shown in Figure 1-3, this step is the core of establishing device ownership. If you already have an account, enter your registered phone number and password, then

tap Next to log in. If you are a new user, tap Register Now at the bottom to proceed to Figure 1-4.

④ Creating a VEILORA OS Account

As shown in Figure 1-4, on the registration screen, enter your phone number and set a strong login password (requires entering twice to confirm). After tapping Register Now, the system will generate exclusive security credentials at the underlying level and strictly bind them uniquely to the current hardware.

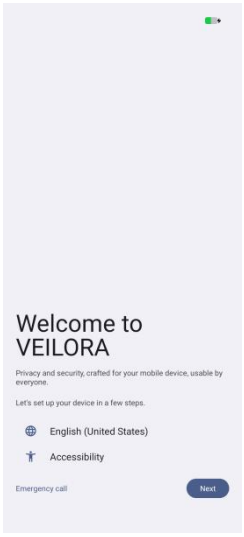


Figure1-1

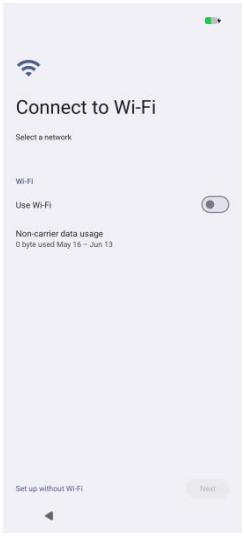


Figure1-2

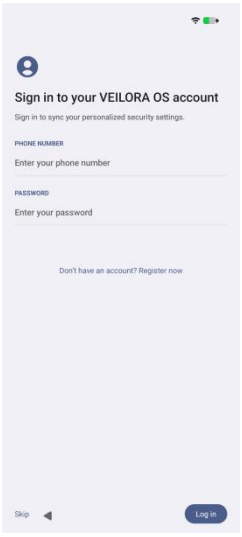


Figure1-3

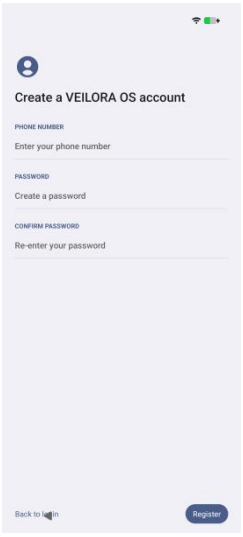


Figure1-4

⑤ Backing Up Core Credentials (Recovery Phrase)

As shown in Figure 1-5, once the account is successfully bound, the system will generate a unique recovery phrase.

Warning: The recovery phrase is your only offline credential for resetting your password, unbinding your device, and recovering data. The system cloud does not retain a copy. Please be sure to accurately write it down on paper and store it in a secure location.

Confirm and Save: After copying it down, check the box for I have safely saved my recovery phrase. The Finish and Return to Login button in the bottom right corner will then unlock. Tap this button to return to the login screen and complete the initial identity activation.

⑥ Verifying Date and Time

As shown in Figure 1-6, the system typically synchronizes the network time automatically. However, please carefully verify that the time zone, date, and time are accurate on this screen. Accurate time parameters are a critical baseline for the system to validate various secure encryption certificates and ensure network communication compliance. Once confirmed, tap Next.

⑦ Location Services Privacy Settings

As shown in Figure 1-7, you can pre-configure low-level location permissions here based on your personal privacy needs. You can independently decide whether to enable switches such as Use Location, Network Location, Wi-Fi Scanning, and Geocoding.

Tip: Completely disabling these options maximizes your geographic stealth (Network Stealth), but it may affect the accuracy of applications like map navigation. Once configured, tap Next.

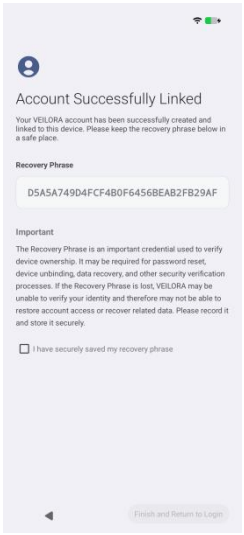


Figure1-5

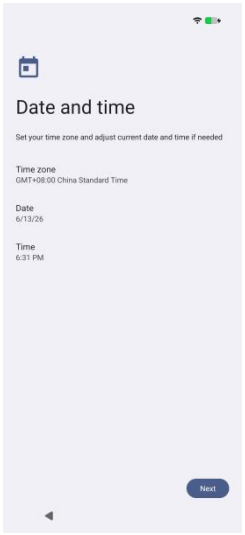


Figure1-6

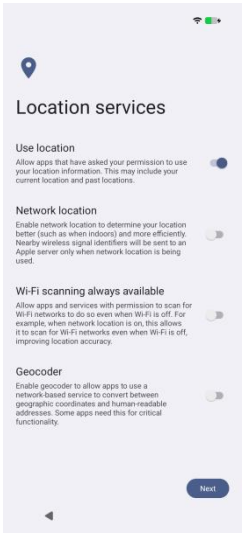


Figure1-7

Setting the System Lock Screen Password (PIN)

After completing the privacy settings above, the system will guide you to the lock screen password setup interface. Follow the on-screen instructions to set your system unlock PIN. This PIN will serve as your core key for accessing the main system space, unlocking the screen, and encrypting local storage.

⑧ Security Preview Patch Settings

As shown in Figure 1-8, by checking the options on this screen, your device will be able to bypass standard update channels to acquire and apply the latest low-level security patches immediately. We recommend enabling this feature. Once configured, tap Next in the bottom right corner.

⑨ Restoring Apps and Data

As shown in Figure 1-9, if you previously used another VEILORA secure smartphone and have a secure backup associated with that account, tap Restore in the bottom right corner for seamless data migration. If you are using this product series for the first time, or if you prefer to start with a brand-new device free of any redundant data, tap Skip in the bottom left corner.

⑩ Gesture Navigation Tutorial and Setup Completion

As shown in Figure 1-10, at the end of the setup assistant, the system will guide you through global swipe gestures (such as swiping from the edge to go back, or swiping up to return to the Home Screen). You can tap Try It in the bottom right corner for an interactive tutorial, or tap Skip in the bottom left corner to exit the setup assistant entirely. Your device is now ready. Welcome to the pure and secure VEILORA OS experience.

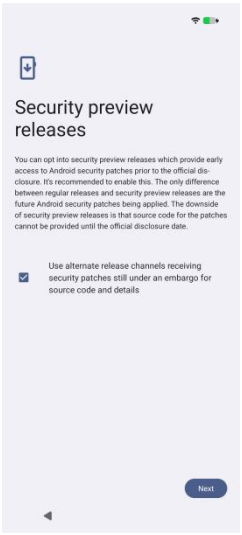


Figure1-8

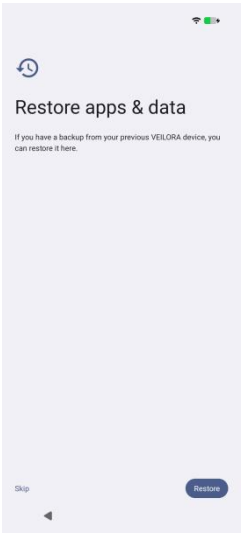


Figure1-9

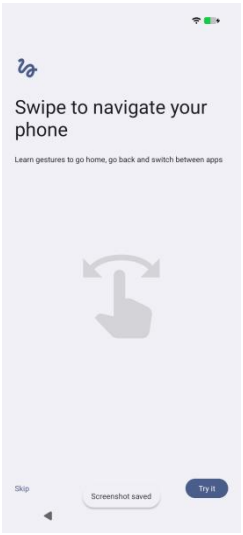


Figure1-10

1.3 System Account Management

The VEILORA secure account is the key to enabling unique device binding, encrypted cloud backup, and remote protection capabilities. Follow these steps to log in and manage your account:

① Accessing Account Management

Open the native Settings app on your device. As shown in Figure 1-11, tap the Not logged in (Tap to log in to your account) item with the blue avatar icon at the very top of the settings list to enter the exclusive personal account management system.

② Account Login and Feature Navigation

As shown in Figure 1-12, on the welcome login screen:

Log In: If you already have an account, enter your registered phone number and password, then tap Log In.

Register: If you are using this device for the first time, tap Register Now in the bottom right corner to proceed to Figure 1-13.

Reset Password: If you have forgotten the password for your existing account, tap Forgot Password? in the bottom left corner to proceed to Figure 1-14.

③ Creating a New Account (Registration)

As shown in Figure 1-13, on the account registration screen, enter the phone number you plan to bind and set a login password that meets the security strength requirements (requires entering twice to confirm). After tapping Register, the system will guide you to generate the critically important recovery phrase (see the subsequent Recovery Phrase Management section for details).

④ Recovering Account Access (Resetting Password)

As shown in Figure 1-14, if you need to recover your account, enter your registered phone number on the password reset screen, along with the recovery phrase you backed up offline during your initial registration. Once the recovery phrase is successfully verified, you can directly set and confirm a new login password.

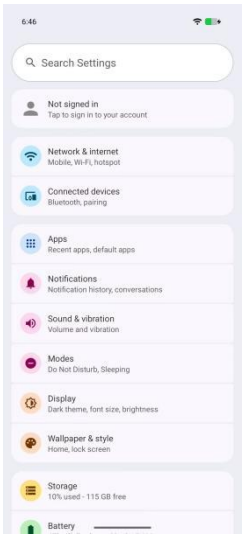


Figure1-11

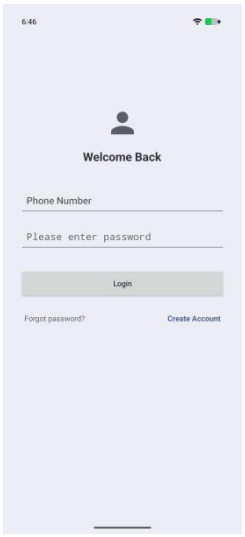


Figure1-12

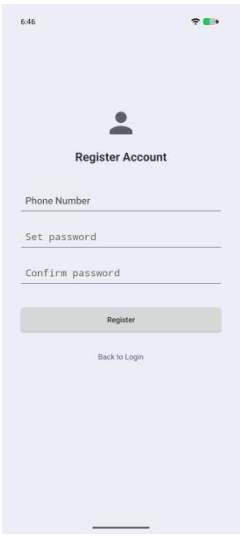


Figure1-13

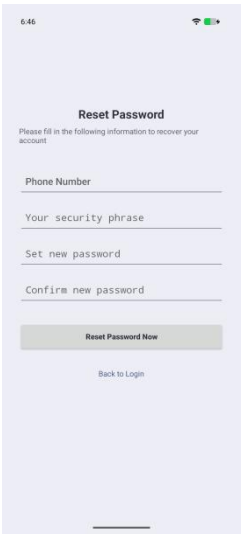


Figure1-14

After successfully logging in, you can comprehensively manage your account profile, security bindings, and core credentials on the Personal Information page.

⑤ Personal Information Homepage

As shown in Figure 1-15, this screen displays your basic account information (Avatar, Nickname, Unique Account ID) and security binding status. From here, you can initiate actions such as changing your password, viewing your recovery phrase, or logging out.

⑥ Changing Your Account Nickname

As shown in Figure 1-16, tap the Nickname field to bring up the modification window. Enter your new name and tap OK to update the display name for your account.

⑦ Unbinding Your Phone Number (Device Release)

If you need to change your account or transfer the device, tap the Phone Number field. As shown in Figure 1-17, the system will prompt a confirmation pop-up. Tap OK and complete the subsequent identity verification to dissolve the strong binding relationship between the current device and your account, which will also log you out automatically.

⑧ Identity Verification for Critical Operations

As shown in Figure 1-18, when performing highly sensitive operations such as viewing your recovery phrase, changing your password, or unbinding your device, the system will mandate the entry of your login password. You can tap the Eye icon to verify the plain text. Once confirmed, tap OK to pass the verification.

⑨ Viewing and Backing Up Your Exclusive Recovery Phrase

As shown in Figure 1-19, upon successful verification, you can view your recovery phrase and its corresponding QR code.

Warning: The recovery phrase is the ultimate credential for regaining access. If you forget your login password and lose your recovery phrase simultaneously, official support cannot reset your account from the backend. Please be sure to properly safeguard your core credentials.

Security Restriction: The screen will display the Remaining Views. Please ensure you securely back it up offline before these attempts are exhausted. Tap Copy and Close to save it to your clipboard with one tap.

⑩ Changing Your Login Password

As shown in Figure 1-20, after tapping Change Password, enter your old password followed by your new password twice. Tap OK to complete the change. If you have forgotten your original password, please refer to the "Recovering Account Access (Resetting Password)" process described earlier.

⑪ Secure Logout

As shown in Figure 1-21, tap Log Out at the bottom of the page and confirm. For maximum privacy protection, logging out will simultaneously and permanently reset all local account cache data on this device. Please ensure important information is synchronized before proceeding.



Figure1-15

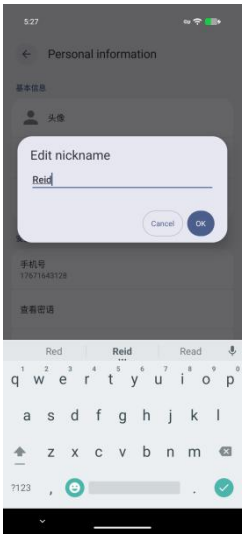


Figure1-16



Figure1-17

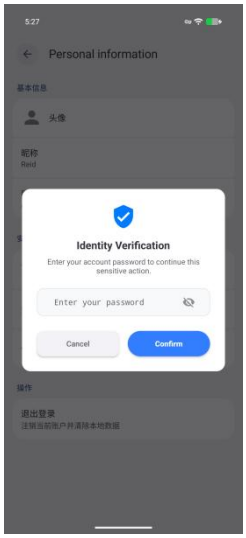


Figure1-18



Figure1-19

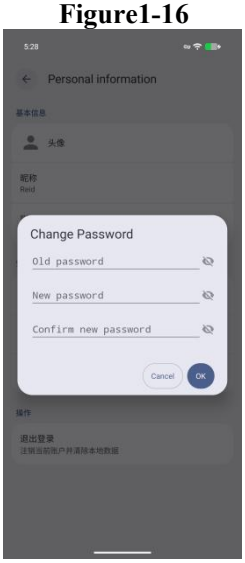


Figure1-20

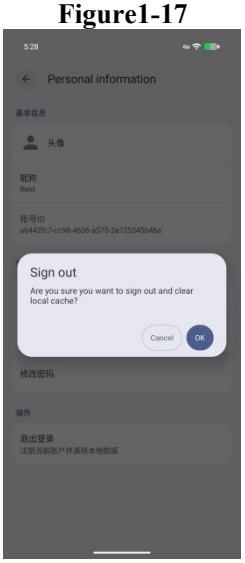


Figure1-21

Helpful Tips:

Offline Storage Only: Your recovery phrase is your only credential for resetting your password. After your initial login, you must write it down on paper or store it in an offline secure hardware device. Never save it as a screenshot in your phone's gallery or send it to others, to prevent irreversible account loss or data breaches.

Log Out vs. Unbind: Log Out only clears the local account cache. Unbind, however, will not only log you out but also reset all records associated with this device from the cloud, disabling protections like remote tracking and One-Tap reset. Please proceed with caution.

1.4 Quick App Installation

To maintain a pristine and secure system environment, the VEILORA smartphone offers a "Featured Apps" quick installation function. With just one tap, you can acquire frequently used office and social applications that have undergone rigorous security and compatibility testing.

① Accessing Featured Apps

As shown in Figure 1-22, open the Device Management app on the Home Screen. At the very bottom of the Control Center panel on the main interface, locate and tap the Featured Apps (One-Tap Install) option.

② Selecting and Executing Batch Installation

As shown in Figure 1-23, upon entering the Featured Apps list page, the system provides a curated selection of essential mainstream software for social networking, payments, shopping, and map navigation.

Single Installation: Tap the Install button to the right of the target app. The system will automatically download and execute the installation from a secure source.

Batch Installation: You can check the selection boxes to the left of multiple apps, or tap Select All in the bottom left corner. Then, tap the blue Install Now (X) button at the bottom. The system will automatically deploy all selected applications in sequence.

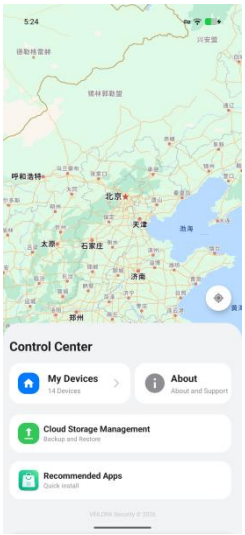


Figure1-22

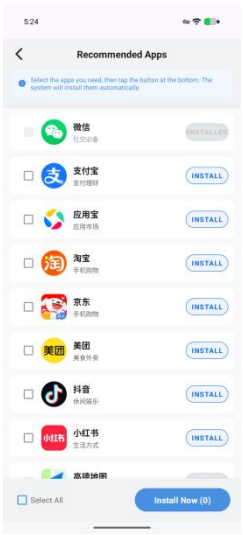


Figure1-23

2. How to Create and Set Up a Private Space

2.1 System-Wide Multi-Level Isolated Encrypted Storage

Physical-Level Multi-Space Isolation: Each space features an independent UID, independently running apps, separate storage partitions, and independent encryption keys. They remain completely isolated and do not interfere with each other.

App Sandbox Isolation: Applications are strictly isolated from one another, significantly mitigating the risk of malicious data theft and data leaks between apps.

File-Level Fine-Grained Encryption: Different users and storage spaces are equipped with distinct encryption keys, achieving precise cryptographic protection down to the individual file and space level.

2.2 Initializing Private Space

The system allows you to use different lock screen passwords to directly enter their corresponding storage spaces. This enables a seamless, instant transition between the Main Space (for daily use) and the Private Space (for highly confidential data).

① Accessing System Settings

As shown in Figure 2-1, tap the Settings icon on the Home Screen. Scroll down the menu list, locate, and tap System. This is the core configuration entry for managing languages, time, and multi-user isolated environments.

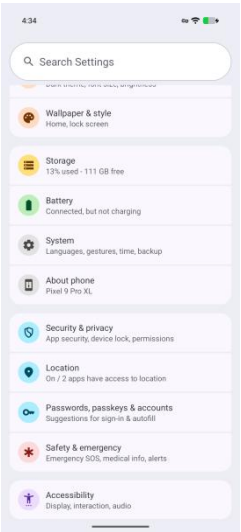


Figure2-1

② Managing User Account Spaces

As shown in Figure 2-2, tap the Users option in the system settings list. On this page, you can visually inspect the status of all storage spaces currently allocated on your device.

③ Accessing the Private Space Entry

As shown in Figure 2-3, locate Private Space in the user list (upon first use, it will be labeled as "Not set up" beneath it). Tap it to enter the detailed feature

configuration page for the Private Space.

④ Space Feature Configuration and Permission Management

As shown in Figure 2-4, on this page you can enable advanced permissions such as Allow running in background and Turn on phone calls & SMS. Once configured, tap the primary item Switch to Private Space to trigger the environment transition.

⑤ Initiating Private Space Setup

As shown in Figure 2-5, a dialog box will prompt you, asking "Set up this user now?". Please tap Set Up Now. The system will then guide you into a completely isolated, brand-new desktop environment. Simply follow the on-screen prompts to complete the setup.

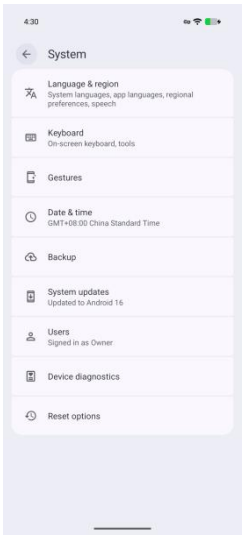


Figure2-2

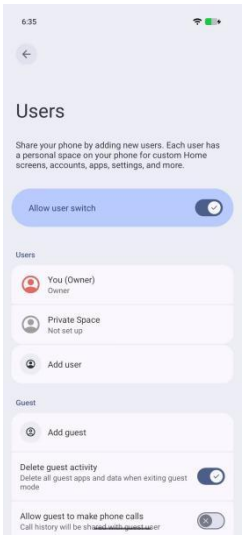


Figure2-3

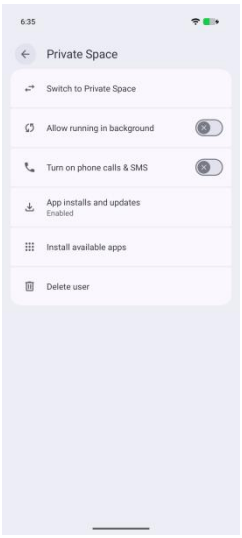


Figure2-4

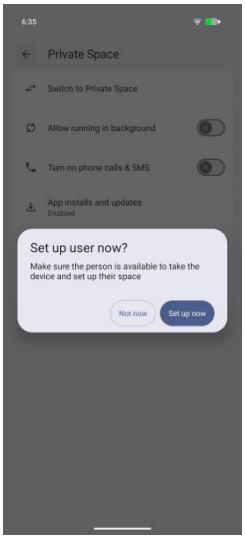


Figure2-5

2.3 Setting Up "Dual PINs" for Space Switching

To achieve ultimate concealment and operational efficiency, VEILORA supports a mechanism that uses distinct passwords to unlock different spaces. By setting different PINs for your Main Space and Private Space, simply entering the respective PIN on the lock screen will prompt the system to automatically recognize and route you to the appropriate space.

① Accessing Security and Privacy Settings

As shown in Figure 2-6, open Settings from the main system interface, scroll

down, and tap the Security & privacy option.

② Selecting Device Unlock

As shown in Figure 2-7, on the Security and privacy management page, tap the Device unlock section.、

③ Enabling Screen Lock Configuration

As shown in Figure 2-8, tap Screen lock (the currently set lock type, such as PIN, is typically displayed beneath it).

④ Setting the PIN and Auto-Confirm Unlock

As shown in Figure 2-9, on the "Choose a new screen lock" interface, tap PIN:

Set Password: Enter a sequence of 6 or more digits.

Suggested Strategy: Set a routine password for the Main Space (e.g., 111111) and a completely distinct, highly secure password for the Private Space (e.g., 888888).

Enable Auto-Confirm (Core Operation): After setting your password, it is critical that you toggle on the Auto-confirm unlock switch below.

Advantage: Once enabled, the moment you finish entering the last correct digit of your PIN on the lock screen, the system will immediately route you into the corresponding space without requiring you to manually tap a confirmation button.

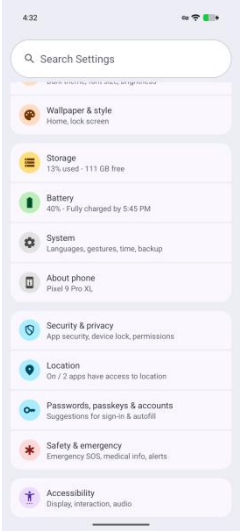


Figure2-6

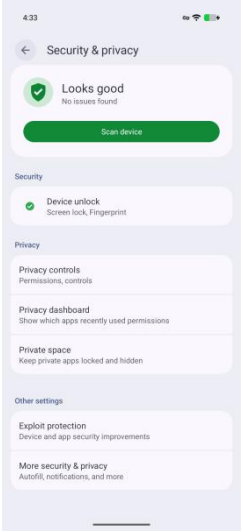


Figure2-7

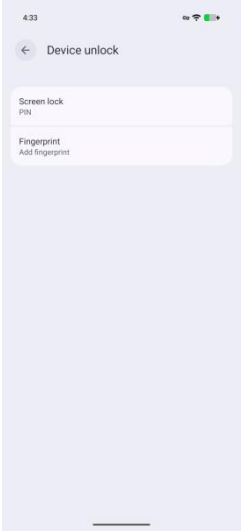


Figure2-8

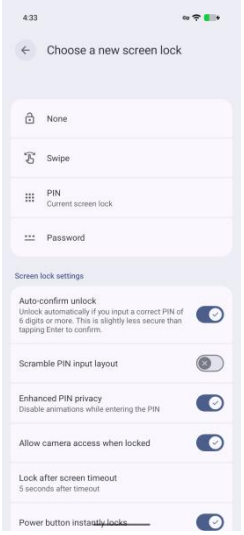


Figure2-9

2.4 Cross-Space File Synchronization Guide (Main Space ➔ Private Space)

The Main Space and Private Space of this system are strictly isolated both physically and logically. When you need to transfer sensitive files from the Main Space to the Private Space for secure keeping, you do not need to rely on external storage devices; you can securely transfer them directly via the system's built-in "One-Tap Sync" feature.

[Phase 1: Initiating Synchronization in the Main Space]

① Selecting Target Files

As shown in Figure 2-10, open the native Files or Gallery app in the Main Space. Browse and locate the sensitive files you wish to transfer (such as the two photos shown in the figure), press and hold to select them.

② Bringing Up Synchronization Options

After selecting the files, tap the ⋮ (three vertical dots) icon in the top right corner of the screen to open the more options menu. As shown in Figure 2-11, select the custom-designed Sync to Private Space option from the drop-down list.

③ Confirming the Synchronization Command

As shown in Figure 2-12, a security confirmation window will pop up in the center of the screen. This step is designed to prevent unintended cross-space data transfer caused by accidental touches. Once verified, tap the Sync button.

④ Viewing Synchronization Feedback

As shown in Figure 2-13, the system will execute data duplication within an underlying encrypted channel. Once the transfer is complete, a prompt reading "Synced X items successfully" will appear at the bottom of the screen, indicating that the files have safely arrived in the Private Space.

[Phase 2: Viewing Files in the Private Space]

⑤ Accessing the Private Space File System

Please switch to the Private Space environment first. As shown in Figure 2-14, open the Files app within the Private Space, tap the ≡ menu in the top left corner to bring up the sidebar, and select your device name (e.g., "Pixel 9 Pro XL") to access the root directory of the internal storage.

⑥ Locating the Sync Reception Directory

As shown in Figure 2-15, locate the system folder named Sync in the root directory list. This folder is the exclusive archive area within the Private Space for receiving data synchronized from the Main Space.

⑦ Accessing the Deep Sync Directory

As shown in Figure 2-16, tap to enter the Sync folder, and proceed to tap the inner Sync subfolder.

⑧ Viewing Files by Original Path

After entering the deep directory, as shown in Figure 2-17, you will find that the system preserves the original directory structure of the files from the Main Space (e.g., Sync > Sync > DCIM > Camera). This design allows you to quickly and accurately retrieve photos or files according to their original organizational logic, even after transferring massive amounts of data.



Figure2-10

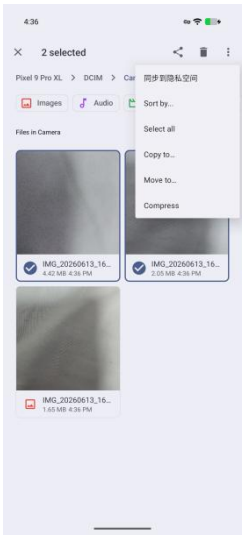


Figure2-11



Figure2-12



Figure2-13

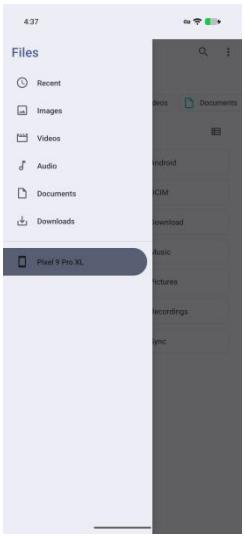


Figure2-14

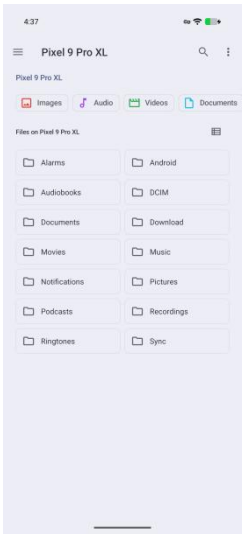


Figure2-15

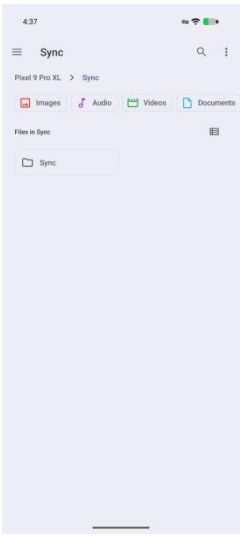


Figure2-16



Figure2-17

3. How to Reduce the Risk of Online Profiling

To counter risks such as endpoint network probing, tracking, attacks, and traffic intrusion, VEILORA dynamically reduces the device's network attack surface through four major mechanisms: Network Stealth, Anti-Tracking Profiling, Proactive Network Attack Protection, and Intelligent Abnormal Traffic Control. This significantly lowers the endpoint's network exposure risk, forging a low-visibility, highly secure network operating environment.

3.1 Anti-Tracking Profiling and Proactive Network Attack Protection

This effectively evades the risks of the device being sniffed, port-scanned, or having its asset signatures captured in both local area networks (LAN) and internet environments It supports manually disabling GPS positioning and base station connections, dynamically shrinking the device's network exposure range, and drastically reducing the probability of the device being discovered or targeted by directed attacks.

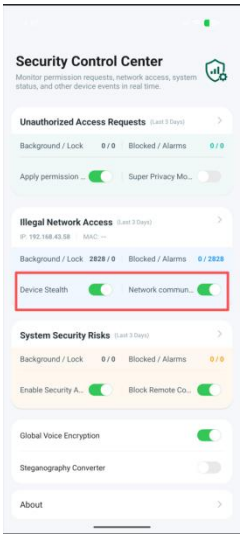


Figure 3-1

As shown in Figure 3-1, locate the Device Stealth switch within the Unauthorized Network Access panel on the home page of the Privacy & Security app.

Default Configuration: For your utmost privacy and security, we strongly recommend keeping this feature enabled by default at all times.

3.2 Intelligent Abnormal Traffic Control

① Enabling Network Communication Control

As shown in Figure 3-2, toggle on the Network Communication Control switch in the Unauthorized Network Access panel on the home page. Once enabled, the system's underlying traffic firewall will comprehensively take over all data packet requests. To view details of abnormal network

② Viewing the Network Risks List

After entering the Network Risks interface (as shown in Figure 3-3), the system will automatically sort the application list based on the frequency of abnormal network connections. You can intuitively see the total number of recent attempts each app has made to connect to external servers, along with their target IP addresses. Through this list, you can quickly isolate suspicious software that frequently consumes traffic in the background while inactive. Tap the card to enter the details page.

③ Executing App-Level Precise Blocking

On the Network Activity Details page of a specific application (as shown in Figure 3-4), you can precisely review the timestamp, target domain/IP, and trigger status of every network connection made by that app.

Precise Control: For applications that do not require internet access, you can navigate to the Permission Control section and enable Deny Access, Deny Background Access, or Deny Screen Lock Access as needed. Once blocking is activated, the system will forcibly sever the application's outbound network communication directly at the underlying network driver level.

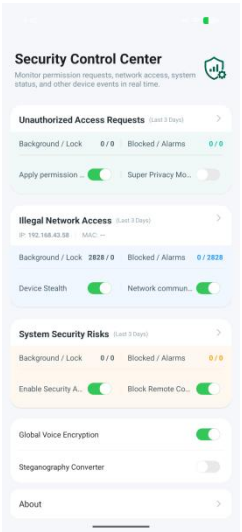


Figure3-2

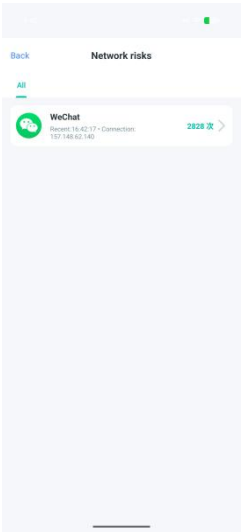


Figure3-3

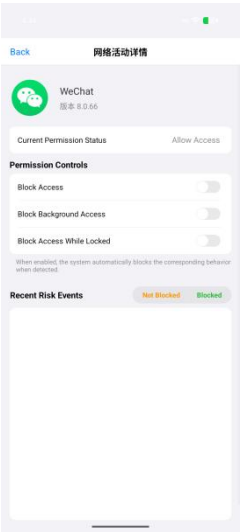


Figure3-4

4. How to Prevent App Privacy Theft

Breaking through traditional static permission authorization models, VEILORA constructs a dynamic privacy protection architecture featuring "Real-Time Auditing, Full-Process Monitoring, Proactive Interception, and One-Tap Protection." This enhances the endpoint's ability to manage privacy permissions across multiple scenarios and states, effectively mitigating security risks such as malicious permission acquisition, background data theft, and unauthorized access by applications.

4.1 App Permission Control and Risk Auditing

The system actively monitors the OS and all third-party apps in real-time—whether running in the foreground, suspended in the background, or during screen lock standby. It tracks access requests and operations involving privacy resources such as contacts, albums, SMS, the clipboard, the microphone, the speaker, location data, Wi-Fi, base stations, and various sensors. This comprehensive monitoring generates detailed permission audit logs, making it easy to trace any privacy-related operations.

During screen lock or when apps reside in the background, the system restricts privacy permission requests based on strict security policies. This significantly lowers the risk of malicious apps acquiring sensitive data in the background without your knowledge, thereby reinforcing privacy protection during standby states.

① Enabling Global Permission Control

As shown in Figure 4-1, on the first screen of the Privacy & Security app, locate the Security Control Center. Find the App Permission Control global switch and toggle it on (it is enabled by default, as shown in Figure 4-2). This operation fully activates the system's low-level permission control capabilities, allowing it to instantly take over and monitor the behavior of all on-device apps to prevent silent privacy theft.

② Viewing the Unauthorized Access Risk List

Tap the Unauthorized Access Requests card above this area to enter the Permission Risks list, as shown in Figure 4-3. On this interface, the system clearly

lists the apps that have recently attempted to invoke sensitive permissions, along with the frequency of their attempts. You can use the top tabs, such as Location, Camera, and Microphone, to filter and quickly identify software suspected of privacy violations.

③ Executing App-Level Precise Blocking

Tap a specific app card to enter its details page. As shown in Figure 4-4, you can execute fine-grained blocking in the Permission Control section, including Deny Access, Deny Background Access, and Deny Screen Lock Access. Once interception is enabled, the system will silently block the app's unauthorized requests directly at the underlying level and generate real-time interception logs in the Recent Risk Records below.

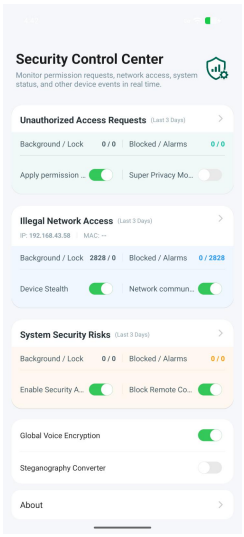


Figure4-1

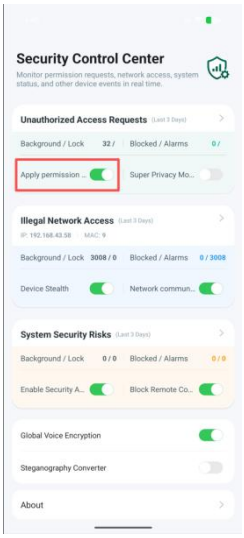


Figure4-2

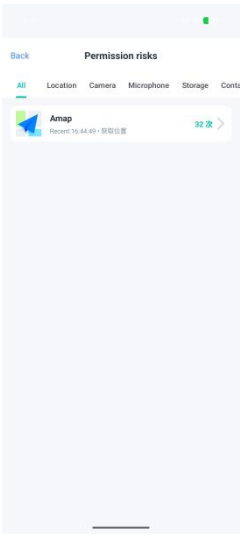


Figure4-3

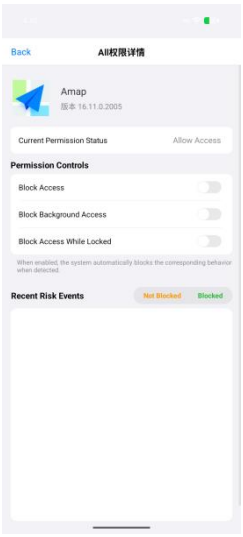


Figure4-4

4.2 One-Tap Super Privacy Mode

Designed for high-frequency, high-privacy scenarios such as confidential meetings, business negotiations, and private environments, this feature allows you to enable Super Privacy Mode with a single tap. It temporarily restricts the ability of all apps on the device to invoke sensitive permissions, mitigating the risk of privacy leaks at the source.

① Triggering Super Privacy Mode

As shown in Figure 4-5, within the Unauthorized Access Requests card area on the home page, toggle on the Super Privacy Mode switch. This feature holds the highest priority for system protection privileges.

② Confirming the Low-Level Fail-safe Warning

As shown in Figure 4-6, the system will prompt a red warning window. Once this mode is activated, the system will forcibly disable the camera, microphone, and GPS location modules at the driver level, completely severing all associated data interaction. Tip: Standard phone calls, video calls, and GPS navigation will be restricted while this is enabled. After acknowledging the prompt, tap Turn On to enter a state of absolute privacy.

③ Exiting Super Privacy Mode

As shown in Figure 4-7, when you leave the sensitive environment and need to restore your phone's normal functions, simply return to this interface and toggle off the Super Privacy Mode switch. The system will reload the underlying hardware drivers, and the device will immediately return to its normal operating state.

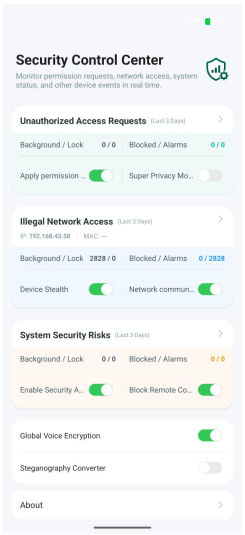


Figure4-5

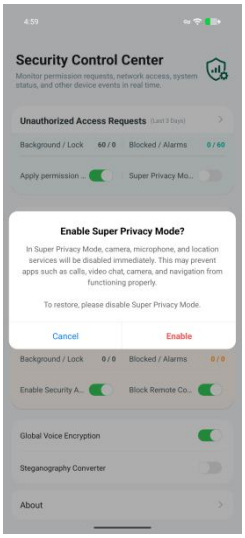


Figure4-6

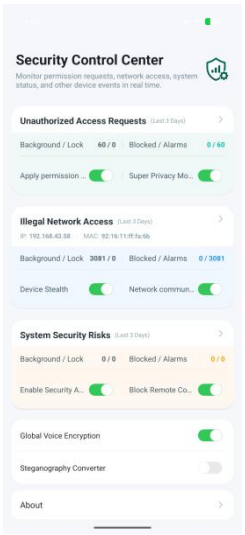


Figure4-7

5. How to Reduce the Risk of Data Leakage Through Third-Party Retention in Instant Messaging

For high-frequency information interaction scenarios such as instant messaging, file transfers, voice calls, and web conferences, the system kernel supports end-to-end encryption. In compatible scenarios, this reduces reliance on modifying third-party applications, lowers the risk of plaintext retention, theft, and leaks on third-party servers, and fundamentally elevates the security of communication data during transmission. (Note: The secure Encrypted Instant Messaging features can only be accessed and utilized within the Private Space.)

5.1 Enabling the Encrypted Conversion Tool

To achieve real-time encryption and decryption of text, voice, and files within third-party applications, you must first enable the system's Encrypted Conversion Tool and grant it the necessary low-level permissions:

① Enabling the Encrypted Conversion Tool

As shown in Figure 5-1, enter the Private Space and open the Privacy & Security app. Locate and tap the Encrypted Conversion Tool option at the bottom of the home page to enable it. Because this feature requires a global floating overlay and manages input method traffic, the system will automatically redirect you to the Accessibility Permissions settings page upon initial activation.

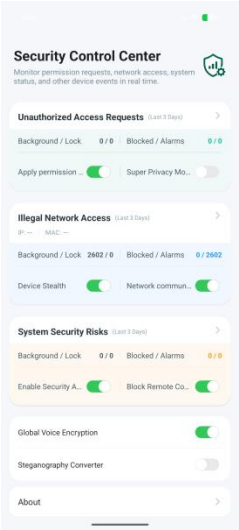


Figure5-1

② Selecting the Service

As shown in Figure 5-2, within the automatically prompted Accessibility service list, locate and tap Privacy & Security.

③ Enabling the Service Switch

As shown in Figure 5-3, after entering the details page, toggle on the switch to the right of Use Privacy & Security.

④ Confirming System Authorization

As shown in Figure 5-4, because this permission involves reading screen content and performing global actions, a high-level security prompt will appear. Read the instructions carefully and tap Allow to authorize the Privacy & Security service to run the underlying encryption engine.

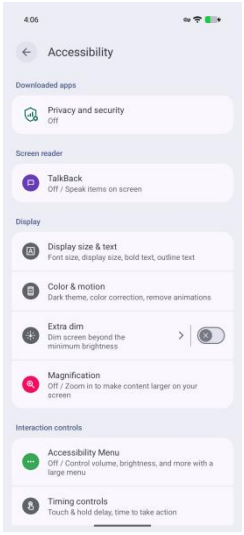


Figure5-2

⑤ Verifying Permission Status

As shown in Figure 5-5, the switch turns blue to indicate it is activated, confirming that the system has successfully granted the necessary underlying operational permissions to the tool.

⑥ Confirming Activation and Verifying the Floating Lock

As shown in Figure 5-6, return to the Privacy & Security app interface. The Encrypted Conversion Tool switch is now toggled on. Simultaneously, a golden floating secure lock icon will appear on the left edge of the screen. You have now completed all prerequisite preparations for communication encryption and can perform encryption operations within any third-party messaging software via this floating lock.

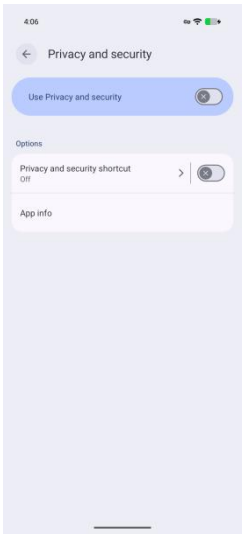


Figure5-3

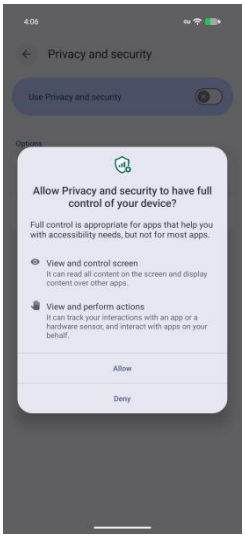


Figure5-4

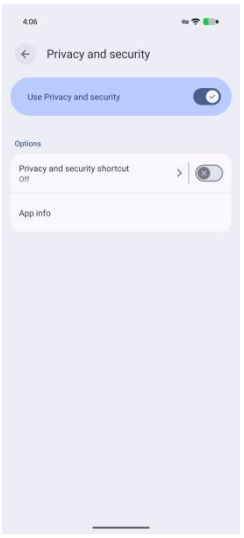


Figure5-5

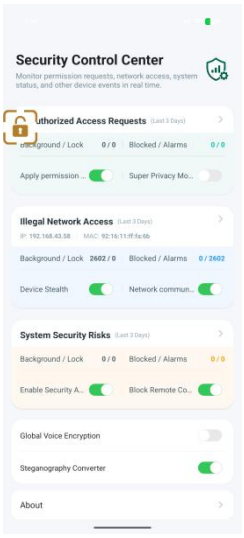


Figure5-6

5.2How to Send Encrypted Messages

Through the Encrypted Conversion Tool, your original chat messages (plaintext) are converted into unreadable, scrambled characters (ciphertext). Even if the messaging application's server is hijacked or chat logs leak, attackers will only see unbreakable ciphertext. Only authorized users with this secure smartphone can restore the original messages on their devices using the dedicated tool.

① Activating the Encrypted Tool Entry

As shown in Figure 5-7, open any instant messaging app and enter a conversation interface. Press and hold the golden floating lock icon on the left side of the screen to bring up the Encrypted Conversion Tool directly over the current screen.

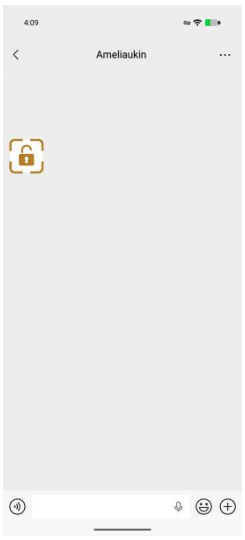


Figure5-7

② Editing Original Plaintext and Generating Ciphertext

As shown in Figure 5-8, in the Encrypted Conversion Tool dialog box, enter the actual message you wish to send (e.g., "Hello"). Once entered, tap the Copy Ciphertext button at the bottom. The system automatically executes strong encryption and saves the generated encrypted string to your system clipboard.

③ Preparing to Paste Ciphertext

As shown in Figure 5-9, tap the × icon in the top right corner to close the tool window and return to the chat interface. Press and hold the native text input field of the messaging app to bring up the system context menu.

④ Pasting Ciphertext into the Input Field

As shown in Figure 5-10, tap Paste from the menu. The scrambled string (ciphertext) generated earlier will be filled into the input field.

⑤ Executing Secure Sending

As shown in Figure 5-11, tap the app's send button to transmit the encrypted message over the network. During this process, any third party or messaging platform server attempting to intercept the data will only obtain this encrypted string, keeping your true communication intent entirely private.

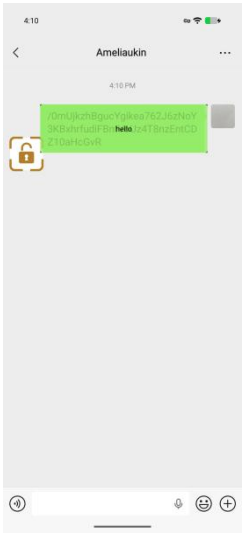


Figure5-12

⑥ Real-Time Message Restoration and Viewing

As shown in Figure 5-12, when you or your contact receive an encrypted message, the secure smartphone's underlying decryption engine automatically recognizes and processes the specific ciphertext format. Utilizing system-level real-time rendering technology, the actual plaintext content (e.g., "Hello" will display as a translucent overlay directly over the original ciphertext. This instant display mode guarantees robust security while maintaining a seamless conversation flow.

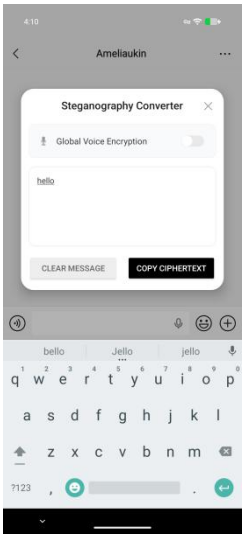


Figure5-8

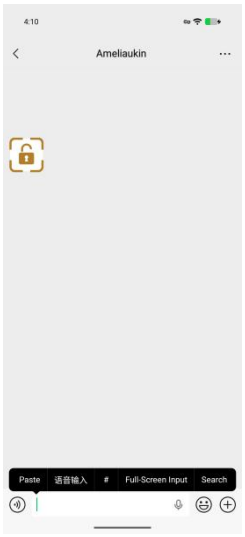


Figure5-9

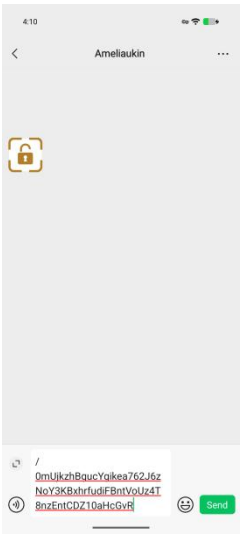


Figure5-10

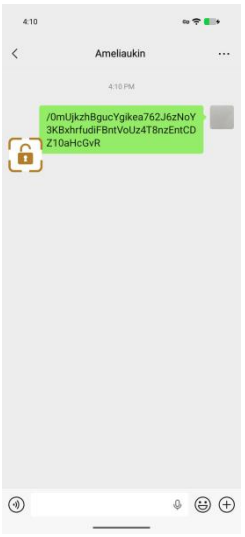


Figure5-11

Note: Real-time ciphertext rendering and decryption currently support WeChat and native SMS. Compatibility with more applications is coming soon.

5.3How to Send Encrypted Files

File transmission supports client-side pre-encryption. Encrypted files are

automatically decrypted once they reach the recipient, minimizing the risk of plaintext files being intercepted or leaked during transit and distribution.

5.3.1 Sending Encrypted or Plaintext Local Files via Third-Party Apps

5.3.1.1 Sending Plaintext Images/Files

① Preparing to Send Files

As shown in Figure 5-13, enter the WeChat conversation interface, tap the + icon, and select the Files function. Core Tip: Observe the golden floating secure lock on the right side of the screen. When the lock icon shows as unlocked, the system is currently in standard plaintext transmission mode.

② Browsing the Plaintext Gallery

As shown in Figure 5-14, under the built-in Gallery tab in WeChat, you can view the original thumbnails of all images on your phone normally, allowing for quick previews and selection.

③ Selecting Plaintext Images

As shown in Figure 5-15, select the image(s) you wish to send and tap Send in the bottom right corner. The images will be transmitted in their standard, unencrypted original format.

④ Selecting Local Files

As shown in Figure 5-16, to send documents or other file types, switch to the Files tab and tap the Select button below.

⑤ Searching the System Directory

As shown in Figure 5-17, the system will invoke the underlying file manager. Here, you can browse the directory structure and select the original plaintext files you want to send.

⑥ Confirming and Completing Plaintext Transmission

As shown in Figure 5-18, after selecting the file, return to the WeChat confirmation interface. The file will display its standard .png or corresponding extension format. Tap Send in the bottom right corner to transfer the file to the recipient without encryption.

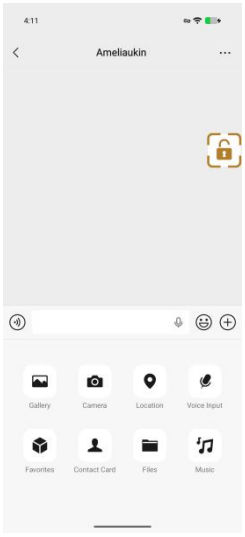


Figure5-13

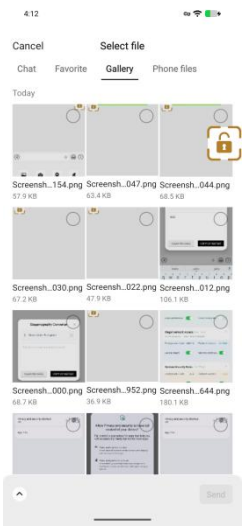


Figure5-14

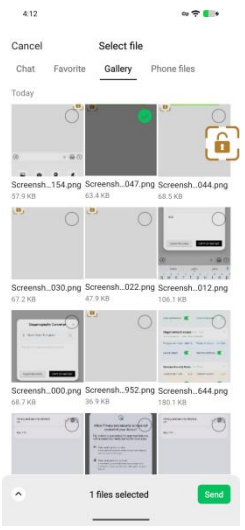


Figure5-15



Figure5-16

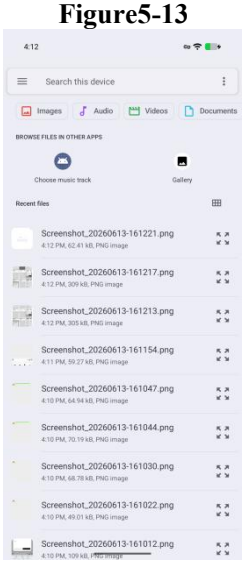


Figure5-17

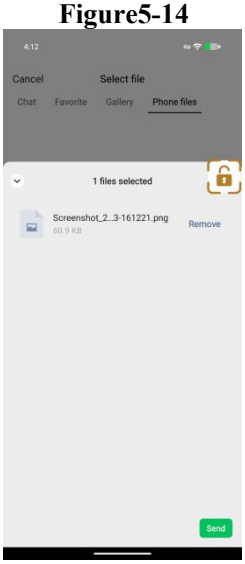


Figure5-18

5.3.1.2 Sending Encrypted Images/Files

① Activating Encryption Mode (Locking)

As shown in Figure 5-19, tap the floating secure lock on the right side of the chat interface to switch it to the closed (locked) state. This indicates that the system's underlying encryption engine has successfully taken over the data interface.

② Automatic Conversion to Encrypted Format

As shown in Figure 5-20, enter the WeChat Gallery tab again. You will notice that the system has automatically applied low-level encryption to all files. Through specialized mechanisms, they remain visible in plaintext on this page for easy selection, while their file name extensions are uniformly changed to .xefc (the system's exclusive encrypted format).

③ Selecting and Sending Encrypted Images

As shown in Figure 5-21, select the target file(s) bearing the .xefc extension and tap the Send button in the bottom right corner. The file will be transmitted as high-strength ciphertext.

④ Accessing the Encrypted File Selection

As shown in Figure 5-22, to send non-gallery files, tap Select under the Files tab.

⑤ Real-Time Low-Level System Encryption

As shown in Figure 5-23, select the target file within the prompted underlying system file manager.

⑥ Confirming the Encrypted Transmission Status

As shown in Figure 5-24, return to the WeChat confirmation interface. You can clearly see that the extension of the file to be sent has automatically changed to .xefc. Once confirmed, tap Send.

⑦ Visual Comparison of Transmission Results

As shown in Figure 5-25, return to the main conversation interface to view the transmission results:

Upper Message (Plaintext): Sent unencrypted, displaying the standard thumbnail and original file name.

Lower Message (Ciphertext): Sent encrypted, displayed in the .xefc format. It cannot be viewed by the platform; only an authorized recipient with the required privileges can decrypt and view it.

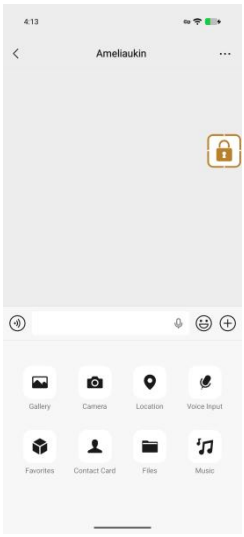


Figure5-19



Figure5-20



Figure5-21

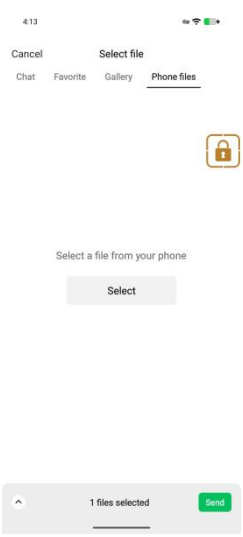


Figure5-22

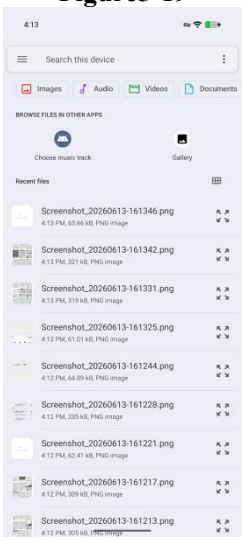


Figure5-23

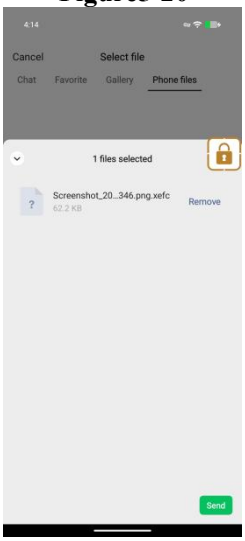


Figure5-24

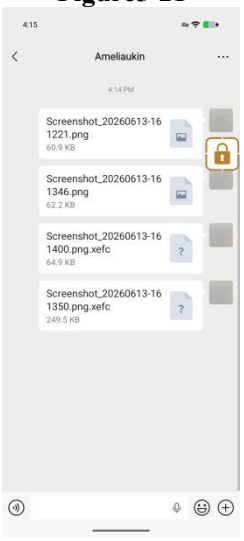


Figure5-25

5.3.2 Sending Files via the File Manager App

5.3.2.1 Sending Plaintext Images/Files

If you need to quickly share non-sensitive photos or documents, please use the standard sharing channel.

① Navigation and Preparation

As shown in Figure 5-26, open the native Files app, tap the menu in the top left corner, and navigate to the target file's directory (e.g., Pixel 9 Pro XL > DCIM > Camera).

② Selecting the File and Identifying the Plaintext Share Icon

As shown in Figure 5-27, press and hold to select the target photo (a blue checkmark will appear). At this moment, two share icons will light up in the top right corner of the screen:

The gray share icon represents the plaintext sharing channel. Tapping this icon brings up the share panel with the original format and file name. Subsequent operations are identical to those on a standard smartphone.

5.3.2.2 Sending Encrypted Images/Files

If the materials you are sending involve core secrets, you must use the red secure encrypted sharing channel.

① Selecting the Target and Invoking the Encrypted Channel

As shown in Figure 5-27, press and hold to select the photo. Tap the specially designed red encrypted share icon in the top right corner. This is the encrypted sharing option to trigger VEILORA's underlying encryption engine.



Figure5-26

② Verifying Encryption Status and Selecting the Channel

As shown in Figure 5-28, on the prompted share panel, please carefully verify that the extension of the file to be shared has indeed changed to .xefc (the system's exclusive encrypted extension). Once automatic encryption is confirmed, select your desired messaging tool from the application list below (e.g., "Send to Chat" in WeChat).

③ Confirming the Recipient and Encrypted Information

As shown in Figure 5-29, select the recipient in the redirected third-party application interface. In the final send preview box, confirm once again that the file name carries the .xefc identifier. Once verified, tap Send.

④ Successful Encrypted Transmission

As shown in Figure 5-30, return to the chat interface. You can see that the encrypted file has been sent successfully. The file remains in an encrypted state

throughout its entire transmission path and on third-party platform servers. It can only be decrypted by an authorized recipient using the exact same model of secure smartphone.



Figure5-27

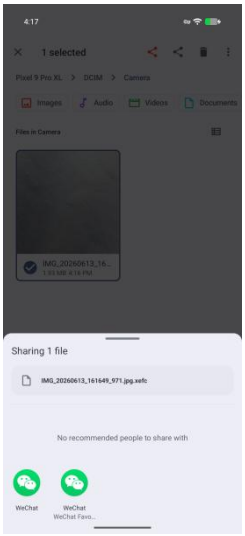


Figure5-28

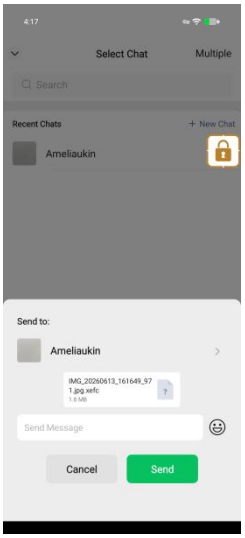


Figure5-29

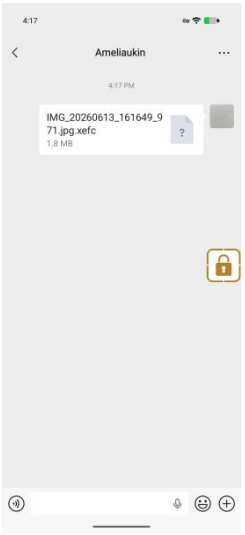


Figure5-30

5.4 Viewing and Browsing Encrypted Files

To view exclusive encrypted files, please follow these standard operational steps:

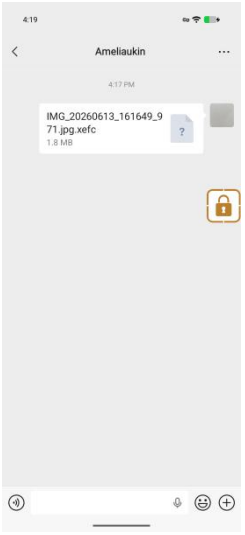


Figure5-31

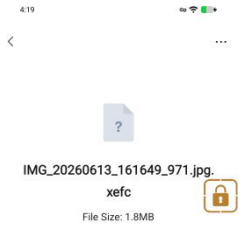
① Triggering Encrypted File Preview

As shown in Figure 5-31, tap the received encrypted file (with the .xefc extension) in the chat interface. The messaging app will enter its system pre-check interface. Because the file is in a high-strength encrypted state, the screen will indicate that it cannot be previewed.

② Invoking the External Secure Opening Method

As shown in Figure 5-32, tap the Open with another app button at the bottom of the screen. At this point, the system's system-level will intercept the request and prompt a list of available secure processing tools.

③ Selecting the Exclusive Secure File Viewer



As shown in Figure 5-33, on the prompted "Open with another app" panel, locate and tap VEILORA Secure Viewer. This is the system's only built-in secure sandbox entry point with decryption privileges.

④ Confirming the Secure Environment Transition



Figure5-32

As shown in Figure 5-34, the system will prompt a secondary confirmation window, warning that you are about to leave the third-party app and open a secure tool. Tap Allow. The system will immediately sever the direct connection with the third-party app and route the encrypted file stream into the protected, isolated secure sandbox for decryption processing.

⑤ Selecting a Viewing Application for the Decrypted File

As shown in Figure 5-35, after the Secure Viewer completes real-time decryption within the sandbox, it will ask which application you want to use to view the decrypted plaintext content.

App Selection: For images or videos, we recommend selecting Gallery; for documents, select WPS or Office.

Recommended Action: After selecting the corresponding app, tap Always. The system will establish a permanent association. When opening similar encrypted files in the future, it will automatically invoke the secure viewer and call the designated app, achieving an "instant-open" experience.

⑥ Successfully Viewing Secure File Content

As shown in Figure 5-36, following real-time processing by the system's underlying secure engine, the actual content of the encrypted file will be help to presented. The viewing process takes place entirely within an isolated memory sandbox, ensuring that the decrypted plaintext content cannot be illegally captured or retained by third-party applications.

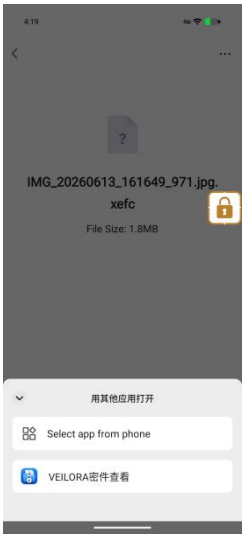


Figure5-33

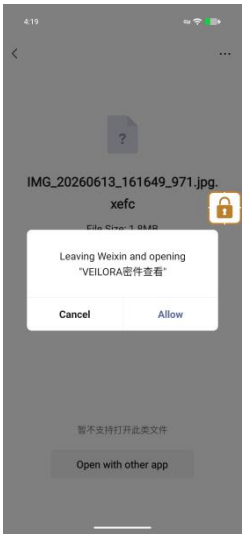


Figure5-34

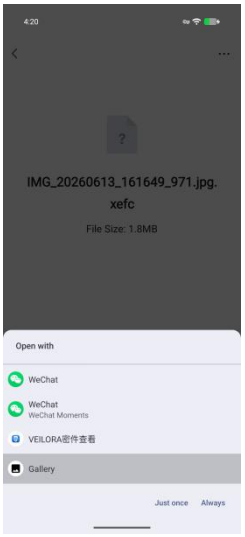


Figure5-35

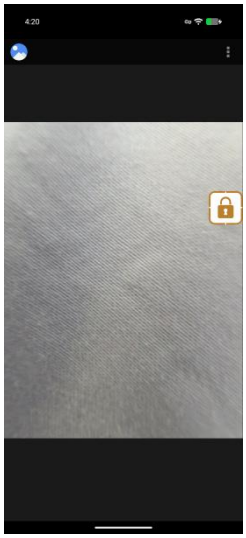


Figure5-36

5.5 How to Make Encrypted Voice Calls

Leveraging native system kernel capabilities, VEILORA automatically encrypts audio capture and decrypts audio playback. This feature supports a wide range of VoIP calls and online conference scenarios, mitigating risks such as eavesdropping, conference content scraping, and plaintext data retention, fundamentally elevating the security of your voice communications.

① Switching to Standard Voice Call Mode (Plaintext)

As shown in Figure 5-37, when the floating secure lock icon shows as unlocked, the system is in standard unencrypted mode.

Status Verification: Tap the icon to toggle it to the unlocked state. In this mode, your calls are transmitted through the messaging app's standard channels, ideal for routine, non-sensitive communication.

② Switching to Secure Encrypted Call Mode (Ciphertext)

As shown in Figure 5-38, tap the floating secure lock icon to change it to the locked state. This activates the system's underlying global voice encryption engine.

Status Verification: When the lock icon is closed, the system automatically intercepts the messaging app's audio stream and applies high-strength, real-time

encryption. Once enabled, you can make encrypted voice calls via third-party apps normally.

③ Enabling Voice Encryption via the Privacy & Security App

As shown in Figures 5-39 and 5-40, while in the Private Space, open the Privacy & Security app. You will find the global voice encryption switch at the bottom of the home page. Toggle this switch to change your voice encryption and decryption modes.

Helpful Tip: This mode effectively prevents conversation content from being illegally intercepted or recorded across network transmission links. For optimal cryptographic protection, it is recommended that both participants use a VEILORA secure smartphone with this mode enabled.



Figure5-37



Figure5-38

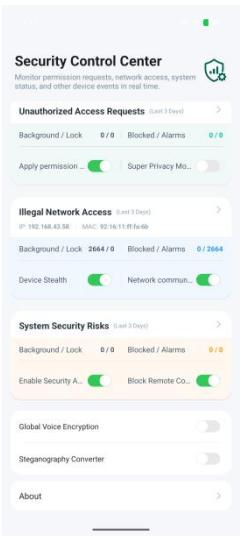


Figure5-39

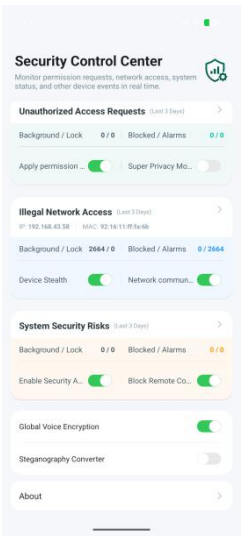


Figure5-40

Helpful Tip: This mode effectively prevents conversation content from being illegally intercepted or recorded across network transmission links. Please note that for optimal cryptographic protection, we strongly recommend both participants use this secure smartphone and enable this mode simultaneously.

6. How to Use the Private Cloud for Encrypted Backups and Restoration

6.1 WebDAV Cloud Space Configuration

Unlike traditional smartphones that restrict you to proprietary manufacturer cloud services, VEILORA's Cloud Space Management supports the universal WebDAV protocol. You can freely choose a self-hosted NAS, a personal server, or a third-party WebDAV-compatible cloud drive as your backup foundation. Through a secure encrypted tunnel, the system automatically synchronizes app data—such as your gallery, contacts, and messages—to your private space, granting you complete data autonomy and secure backups.

① Accessing Cloud Space Management

As shown in Figure 6-1, open the Device Management app on the Home Screen. In the Control Center panel below, tap the Cloud Space Management option. This module serves as the unified hub for managing remote storage nodes and automated backup strategies.

② Cloud Space Status Overview and App Configuration

As shown in Figure 6-2, upon entering the main page, you can view the name of the cloud space currently in use (such as the default "VEILORA") and its connection status at the top. On this page, you can toggle the switches to independently select the data categories you wish to back up (e.g., Gallery, Contacts, Messages, Call Logs). Tap the Manage button to access advanced node configurations.

③ Managing the Cloud Space List

As shown in Figure 6-3, this interface displays all linked cloud storage nodes. To add a new private storage space, tap the blue + icon on the right.

④ Selecting the Cloud Space Protocol

As shown in Figure 6-4, the system will prompt a protocol selection menu. Tap to select WebDAV. This is a universal, standard network storage protocol that seamlessly supports most self-hosted NAS devices (such as Synology or QNAP) or WebDAV-compatible third-party cloud storage services.

⑤ Configuring Server Connection Parameters

As shown in Figure 6-5, accurately enter your cloud storage credentials on the setup interface:

Space Name: Customize a recognizable profile name.

Server URL: Enter the WebDAV address (must include the protocol prefix and port number, e.g., http://ip:port/dav).

Account/Password: Enter the corresponding login credentials.

Once completed, tap Verify & Add. The system will automatically perform a handshake connection test.

⑥ Setting the Default Storage Node

As shown in Figure 6-6, tap the target space card from the list of linked spaces. From the pop-up menu, select Set as Default Cloud Space. Once successfully configured, all subsequent automated encrypted backup commands from the system will be routed directly to this space. You can also execute a Delete Cloud Space action here.

⑦ Designating the Remote Backup Root Directory

As shown in Figure 6-7, enter the directory tree interface of the specified space, browse to, and open your pre-configured backup folder (such as the backup directory). Once the path is verified, tap Set as Backup Directory in the top right corner. Your private encrypted backup channel is now officially established, and critical local data will automatically synchronize to this secure zone according to your configured policy.

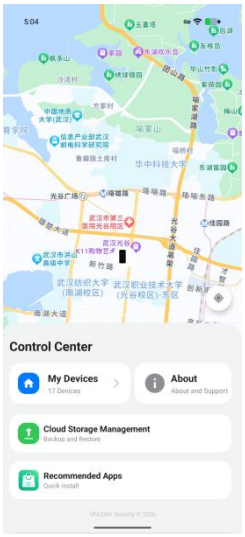


Figure6-1

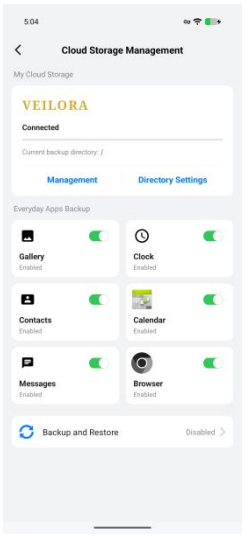


Figure6-2

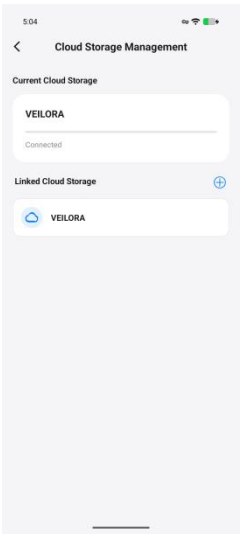


Figure6-3

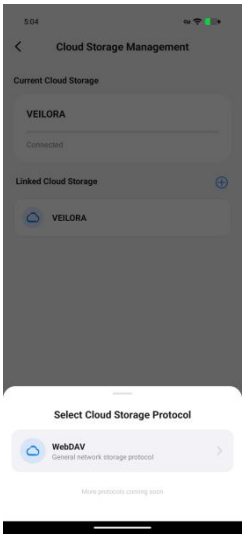


Figure6-4

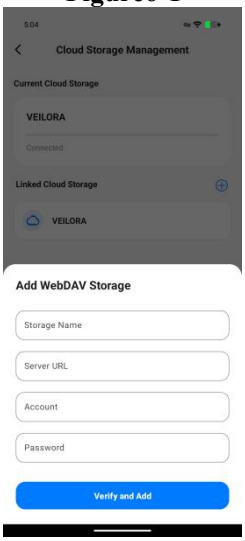


Figure6-5

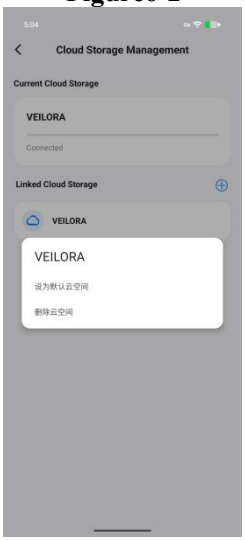


Figure6-6

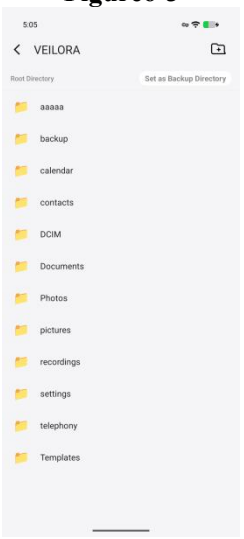


Figure6-7

End-to-End Encryption: All data uploaded to your private cloud is encrypted locally the instant the screen turns off. Even if your WebDAV server itself is compromised, unauthorized actors cannot decrypt the contents of your backup files without your device-specific keys.

6.2 Setting Up Automatic/Manual Backup Schedules

The Backup & Restore feature provides both automatic and manual data backup modes. The system employs a "silent backup" logic, meaning that when the device is connected to power, the screen is locked, and Wi-Fi is connected, it will automatically back up designated applications, ensuring the process never disrupts your daily usage. You can also initiate a manual backup at any time to preserve an instant snapshot of

your current critical data.

Once your private cloud storage node is configured, you can set up an automated backup schedule to ensure that if your device is lost or damaged, your data can be fully restored via an encrypted cloud snapshot.

① Accessing Cloud Space Management

As shown in Figure 6-8, launch the built-in Device Management app. Tap Cloud Space Management in the Home Screen Control Center. This module serves as your unified hub for managing all remote storage paths and executing data synchronization tasks.

② Configuring Basic Backup Items

As shown in Figure 6-9, first ensure that the cloud space at the top displays a "Connected" status.

Quick Sync: In the Daily App Backup list, you can check the boxes to back up core baseline data like Gallery, Contacts, Messages, and Call Logs with one tap.

Advanced Settings: Once baseline items are selected, tap the Backup & Restore item at the very bottom of the page to enter the automated schedule configuration page.

③ Configuring Backup Schedules and Manual Execution

As shown in Figure 6-10, this interface gives you comprehensive control over backup operations:

Activate Automatic Backup: Toggle on the Back up this device switch. The system will silently execute background backups when the device is idle, connected to power, and on Wi-Fi.

Frequency Control and Manual Backup: Define the interval via Backup frequency (e.g., once every 7 days), or tap the Back up now text to immediately trigger a manual upload.

Cross-Device Version Management: In the All device backups list, you can visually track the backup sizes and timestamps stored in the cloud for this device as

well as other linked devices under the same account.

④ Granular Content Selection

As shown in Figure 6-11, tap Backup options on the previous page to enter the granular configuration interface.

Customized Content: You can tailor selections for system settings, calendar, voice recordings, and even specific third-party application data.

Storage Optimization: This precise configuration allows you to prioritize backing up core confidential business data, helping you manage the storage capacity of your private WebDAV space more effectively.

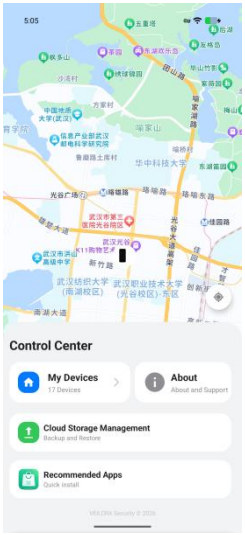


Figure6-8

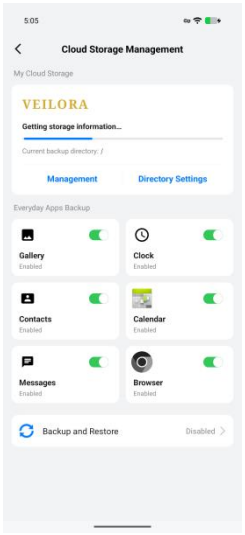


Figure6-9

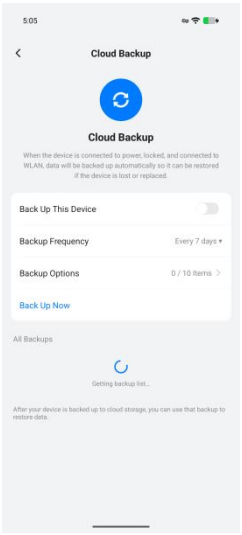


Figure6-10

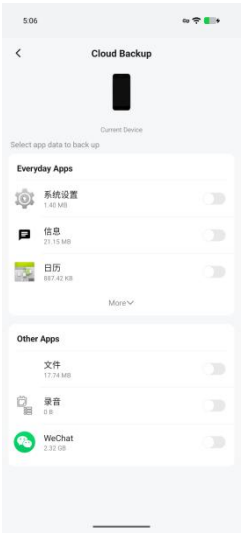


Figure6-11

Helpful Tip: All backup data undergoes strong encryption at the system's system-level during transmission. This ensures that even if cloud storage content is unlawfully accessed, it cannot be decrypted.

6.3 Local Data Recovery Process

This section covers the cloud data recovery steps, recovery scope, progress tracking, and exception handling during device resets or device migration scenarios.

① Accessing Cloud Space Management

As shown in Figure 6-12, open the Device Management app and tap Cloud Space Management on the main interface. This module acts as the access interface to your private cloud assets.

② Entering Backup & Restore Settings

As shown in Figure 6-13, first confirm that the cloud space status at the top displays "Connected." Then, tap the Backup & Restore option at the bottom to enter the data restoration interface.

③ Selecting the Source Device

The system supports multi-device backups sharing a single cloud space. As shown in Figure 6-14, the All device backups section lists all endpoint records currently stored in your WebDAV space. Tap the target device from which you wish to extract data (e.g., Pixel 9 Pro XL).

④ Selecting a Historical Snapshot

As shown in Figure 6-15, enter the backup management page for the designated device to view all historical snapshots. Select your desired backup entry from the Other backups list based on your timeframe preference.

⑤ Selecting Data Items to Restore

As shown in Figure 6-16, on the data selection interface, you can perform on-demand restoration:

Granular Selection: Select the specific application data you wish to restore (e.g., Gallery, Contacts, System Settings).

Execute Restore: Verify the number of selected items and total file size, then tap the blue Restore Selected Data button at the bottom.

⑥ Confirming the Restoration Risk

As shown in Figure 6-17, a red warning dialog box will prompt you, asking "Restore data?".

Data Overwrite Policy: Please note that the restoration process will overwrite existing data on your device with the cloud data. This action is irreversible. Ensure

you are in a secure environment with sufficient battery level, then tap Continue.

⑦ Entering the Recovery Phrase for Verification

To prevent unauthorized extraction of backup data, the system will trigger a high-level identity verification check.

Verify Identity: As shown in Figure 6-18, enter the unique recovery phrase of the device that owns the backup data (the phrase you copied down during the initial setup).

Begin Restoration: Tap Verify. Once validated, the system will instantly initiate the cloud download and execute real-time stream decryption, automatically completing the local data overwrite and recovery.

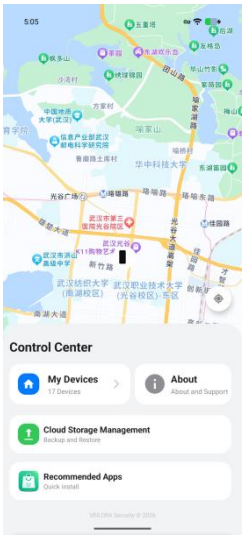


Figure6-12

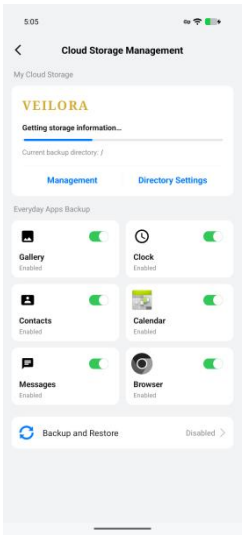


Figure6-13

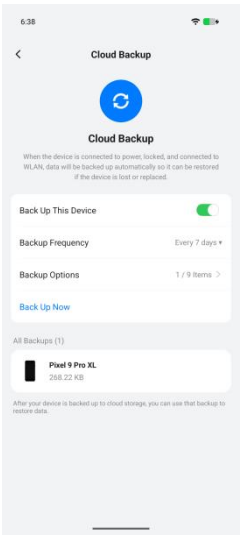


Figure6-14

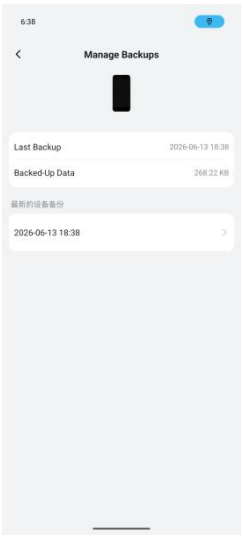


Figure6-15

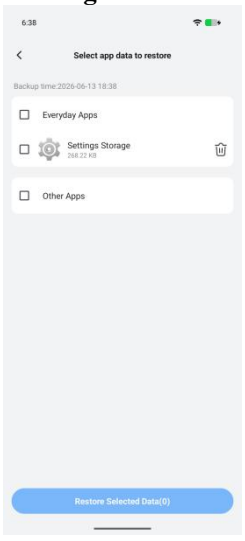


Figure6-16

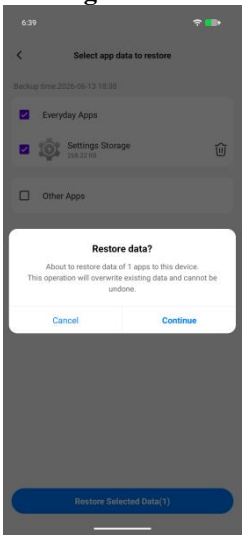


Figure6-17

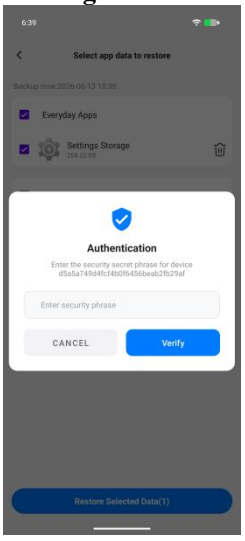


Figure6-18

7. How to Reinforce System Security

Driven by the system's on-device secure intelligent kernel, VEILORA moves beyond traditional passive defense models. By enhancing self-learning security capabilities, abnormal behavior recognition, and real-time interception, the system actively counters unknown threats and emerging exploits while continuously iterating its security defenses.

① Enabling the On-Device Security Agent (AI Proactive Defense)

As shown in Figure 7-1, open the Privacy & Security app. Within the System Security Risks card on the home page, locate the Enable Security Agent switch (enabled by default). Once turned on, the local AI model analyzes system command streams and application behaviors in real time, intelligently identifying and intercepting zero-day attacks to achieve autonomous, proactive defense.

② Enabling System-Level Anti-Remote Control

As shown in Figure 7-2, within the same panel, toggle on the Block Remote Control switch (enabled by default). This feature cuts off all remote assistance protocols, screen-sharing streams, ADB debugging interfaces, and simulated touch behaviors directly at the underlying driver level, ensuring your device cannot be covertly manipulated over the network.

③ Accessing the System Risk Management Interface

As shown in Figure 7-3, tap anywhere on the System Security Risks card to navigate into the detailed system security risk list. Through this entry point, you can audit and trace various low-level security events on your device.

④ Real-Time Scanning and Multi-Dimensional Risk Auditing

As shown in Figure 7-4, upon entering the details page, the top navigation bar categorizes threats into specialized dimensions such as High-Risk Commands, File

Risks, Network Risks, and Process Risks.

System Health: Under normal conditions, the lists will remain empty, indicating that system running in secure and stable condition..

Automatic Interception: If malware attempts privilege escalation, invokes high-risk instructions, or spawns unauthorized processes, the system will immediately issue an alert here and execute an automatic block to preserve the system baseline.

On-Device Execution: The security agent operates entirely locally on your device. It never uploads any of your behavioral data to the cloud, help to balancing intelligent defense with uncompromising privacy protection.

In addition to active monitoring, VEILORA provides system-level exploit mitigation strategies. By hardening hardware interfaces and low-level memory management, it establishes a rugged foundation against zero-day attacks.

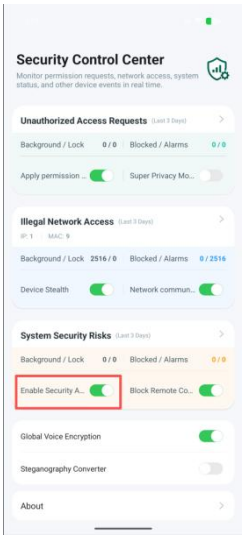


Figure7-1

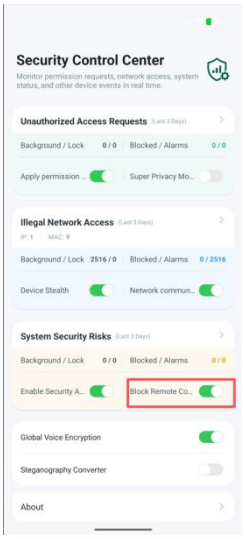


Figure7-2

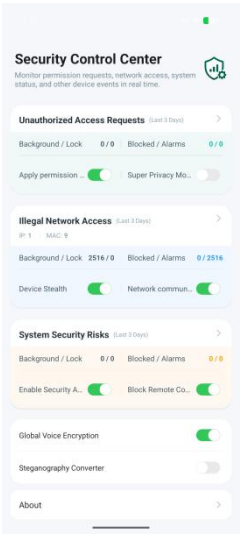


Figure7-3

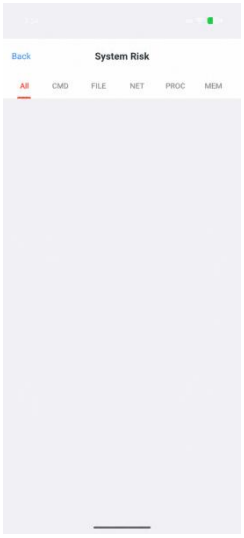


Figure7-4

In addition to active monitoring, VEILORA provides system-level exploit mitigation strategies. By hardening hardware interfaces and low-level memory management, it establishes a rugged foundation against zero-day attacks.

① Accessing System Security and Privacy Settings

Open the native Settings app on your device, locate and tap Security & privacy, as shown in Figure 7-5. This page is the centralized hub for native system security capabilities, displaying your device's overall compliance status and foundational

protection options.

② Accessing Exploit Protection

As shown in Figure 7-6, scroll to the bottom of the Security & privacy page and tap Exploit protection under the Other settings section. This module contains multiple advanced hardening toggles targeting hardware ports, wireless connections, and the application execution environment.

③ Hardware Interfaces and System-Level Security Configuration

As shown in Figure 7-7, after entering the details page, you can define in-depth policies for physical and network connections:

USB-C Port Protection: We recommend keeping this set to Charge only when locked. This feature severs the USB data link at the low level when the screen is locked, preventing unauthorized data extraction via physical hardware connections.

Auto-Reboot: Set a fixed reboot schedule (e.g., every 18 hours). Periodic reboots forcibly flush non-persistent malicious scripts from memory and return cryptographic system keys to a cold-encrypted state.

Wireless Connection Control: You can configure Wi-Fi or Bluetooth to turn off automatically when idle, minimizing the device's wireless attack surface.

④ App-Level Memory and Dynamic Code Protection

As shown in Figure 7-8, within the App-level exploit protection area at the bottom of the page, you can configure deep sandbox defenses (keeping the default configuration is highly recommended):

Hardened Memory Allocator: Utilizes technologies such as Memory Tagging Extensions (MTE) to intercept exploit attempts like buffer overflows targeting application vulnerabilities in real time.

Dynamic Code Loading Protection: Strictly governs the behavior of third-party apps executing unauthorized instructions dynamically in memory, effectively blocking covert injection paths for Trojans and malware.

Secure Process Startup: When enabled, the system executes integrity checks on every newly launched app process, ensuring its core code remains untampered with.

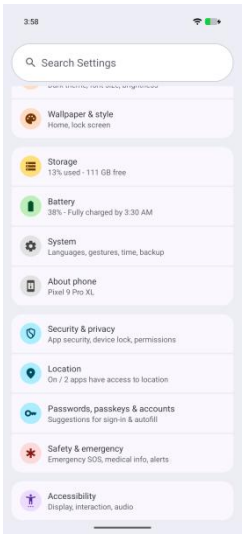


Figure7-5

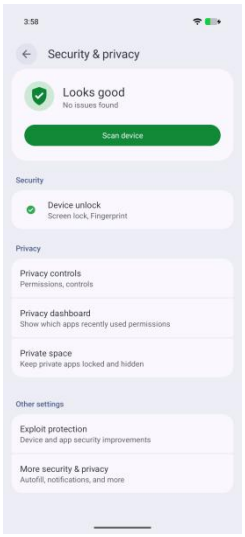


Figure7-6

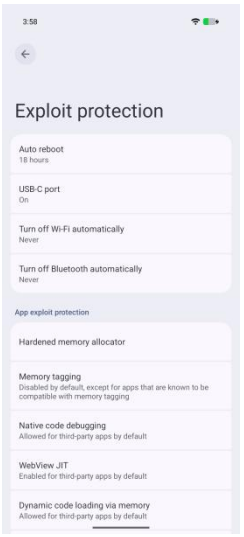


Figure7-7

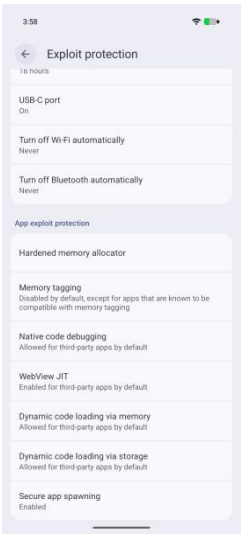


Figure7-8

8. How to Perform an Emergency Reset

Designed for extreme and exceptional scenarios such as device loss or physical duress, VEILORA builds a three-tier cryptographic emergency system combined with rapid emergency response capabilities. This allows you to instantly elevate the device's security level, significantly mitigating the risk of core privacy data being unlawfully acquired.

Standard Unlock Key (PIN): Used for routine device unlocking and seamlessly switching between dual-domain spaces, ensuring normal daily usage. Private Space Reset Key: Upon entering this key, the user appears to normally access the standard Main Space, while the system simultaneously and irreversibly wipes the Private Space back to its factory state. Device Reset Key: Triggers an immediate factory reset of the entire device, achieving the highest echelon of data protection.

8.1 How to Reset the Entire Device

8.1.1 Device Reset Password Setup

The Device Reset Password is an emergency feature tailored for extreme security scenarios. When facing duress or critical situations, entering this pre-set password triggers the system to immediately enter a designated security state (such as data erasure or privacy concealment), ensuring core sensitive information is not compromised. Setup steps are as follows:

① Accessing Security and Privacy Settings

As shown in Figure 8-1, tap the Settings icon on the Home Screen to enter the main system settings menu. Locate and tap the Security & privacy option. This module is the core entry point for managing device locks, biometrics, and privacy permissions.

② Expanding Advanced Security Options

As shown in Figure 8-2, scroll to the bottom of the Security & privacy page and tap More security & privacy under the Other settings section to access deeper system hardening options.

③ Accessing the Emergency Protection Entry

As shown in Figure 8-3, scroll down the More security & privacy page and tap Emergency protection under the Security category. This feature is designed specifically for extreme emergencies, providing your final data protection barrier.

④ Configuring the Device Reset Password

As shown in Figure 8-4, tap Device Reset Password on the Emergency protection page.

Identity Verification: The system will first verify your current lock screen PIN to ensure the action is authorized by you.

Set Reset Password: Upon successful verification, follow the on-screen prompts to set your exclusive reset password.

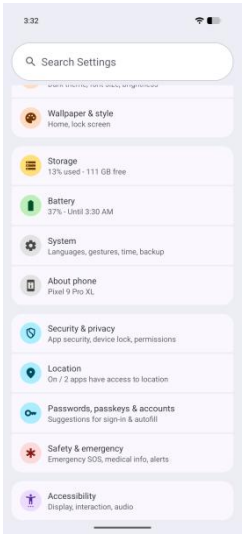


Figure8-1

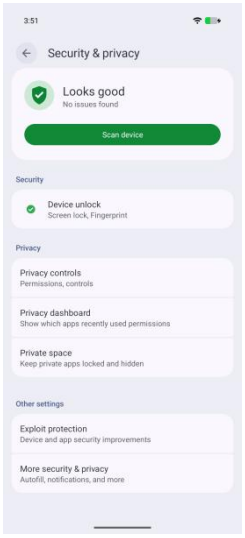


Figure8-2

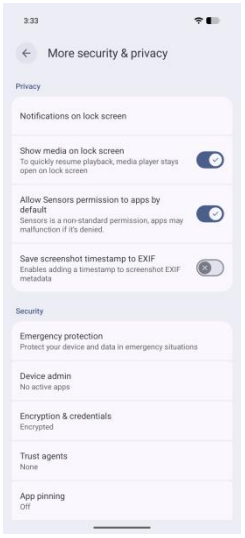


Figure8-3

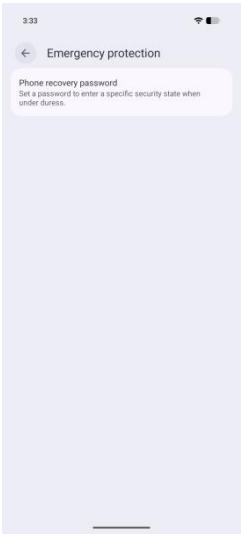


Figure8-4

Helpful Tip: Please ensure this password is completely distinct from your standard daily unlock password. Once set successfully, entering this Device Reset Password during moments of security threat will trigger a factory reset of the device, achieving the highest level of data protection.

8.2 How to Reset the Private Space

8.2.1 Private Space One-Tap Reset Setup

The Private Space One-Tap Reset is a "digital wipe" switch specifically designed to counter sudden threats. Once enabled, users do not need to navigate complex menus; simply pressing and holding the Power Button to bring up the power menu allows you to immediately execute a data erasure command for the Private Space. Setup steps are as follows:

① Accessing Security and Privacy Settings

As shown in Figure 8-5, open Settings from the main system interface, locate and tap the Security & privacy option near the bottom of the list.

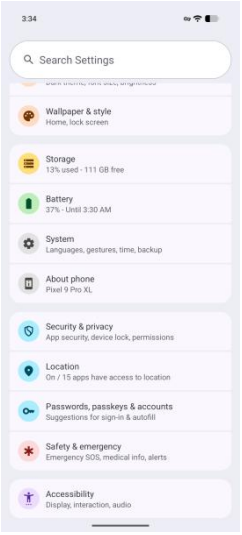


Figure8-5

② Accessing More Security Settings

As shown in Figure 8-6, scroll to the very bottom of the Security & privacy page and tap More security & privacy under the Other settings section.

③ Enabling the Emergency Protection Entry

As shown in Figure 8-7, scroll down to the Security section and tap the Emergency protection option. This feature represents the device's last line of defense for protecting core data under extreme circumstances.

④ Activating the "One-Tap Reset" Switch

As shown in Figure 8-8, toggle on the switch next to One-Tap Reset on the Emergency protection page.

Functional Principle: Once enabled, the system will add a new quick command named One-Tap Reset to the underlying power management menu, allowing you to trigger protection seamlessly without unlocking the screen.

⑤ Bringing Up the Power Menu and Executing Reset

As shown in Figure 8-9, when you need to execute emergency private space recovery:

Invoke Menu: From any device state (including locked screen, screen off, or screen on), press and hold the Power Button.

Execute Reset: On the prompted power menu, tap and hold the One-Tap Reset icon in the bottom right corner.

Execution Result: Upon execution, the system will immediately and silently reset all confidential data and settings within the Private Space, ensuring core privacy cannot be accessed by third parties.

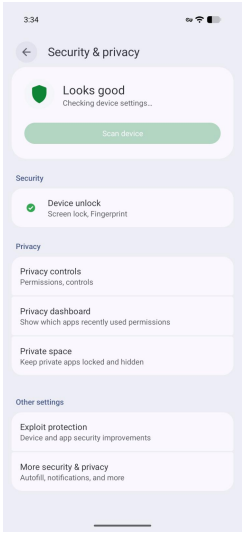


Figure8-6

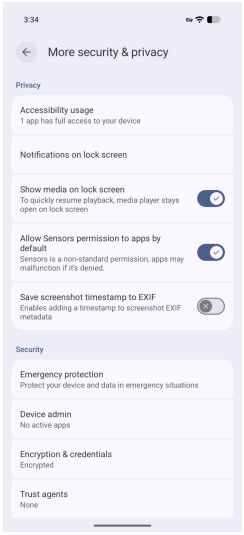


Figure8-7

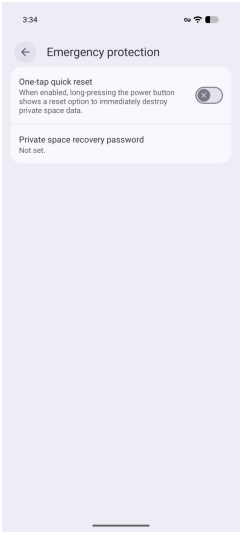


Figure8-8

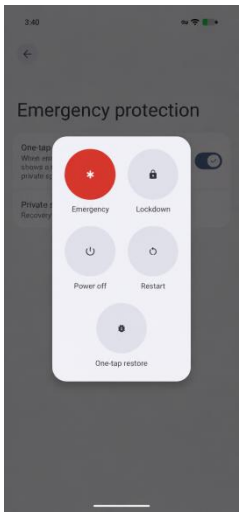


Figure8-9

Operational Warning: In an emergency, pressing and holding this button will immediately wipe all Private Space data according to the pre-set logic. This action is irreversible. Please use it with extreme caution—only when data is safely backed up or when genuinely facing a severe security threat.

8.2.2 Private Space Reset Password Setup

The Private Space Reset Password (Duress PIN) is a special 6-digit code. Unlike standard unlock passwords, when you enter this specific PIN on the lock screen, the system will seemingly authenticate you normally into the Main Space. However, concurrently and entirely in the background, it will immediately execute pre-set commands to reset Private Space data. The entire process requires no secondary confirmation, offering extremely high concealment and a rapid response time. Please follow these steps to configure it:

① Accessing Security and Privacy Settings

As shown in Figure 8-10, tap the Settings icon on the main system interface.

Locate and tap the Security & privacy option near the bottom to enter the system's comprehensive security management page.

② Accessing More Setting Options

As shown in Figure 8-11, scroll to the very bottom of the Security & privacy page and tap More security & privacy under the Other settings section.

③ Locating the Emergency Protection Entry

As shown in Figure 8-12, scroll down the More security & privacy page. Locate and tap the Emergency protection item under the Security section. This is the entry for emergency recovery management.

④ Initiating Reset Password Setup

As shown in Figure 8-13, on the Emergency protection page, the Private Space Reset Password is displayed as "Not set up" by default. Tap this option to officially launch the setup wizard for the reset password (silent duress PIN).

⑤ Setting the 6-Digit Duress PIN

As shown in Figure 8-14, the system redirects to the "Set Duress PIN" interface. Please enter a unique 6-digit sequence here.

Security Recommendation: To ensure the concealment and precision of the emergency trigger, this password must be completely different from your standard lock screen password and your Private Space access password. Using overly simple or sequential numbers is strictly prohibited.

⑥ Re-entering for Confirmation

As shown in Figure 8-15, follow the on-screen prompts to re-enter the 6-digit sequence you just configured for verification. Once confirmed, tap the Confirm button at the bottom.

⑦ Verifying Setup Status

As shown in Figure 8-16, upon successful configuration, a "Setup Successful" floating notification will appear at the bottom of the screen. Returning to the main

Emergency protection page, you will see the option has updated to "Reset password set".

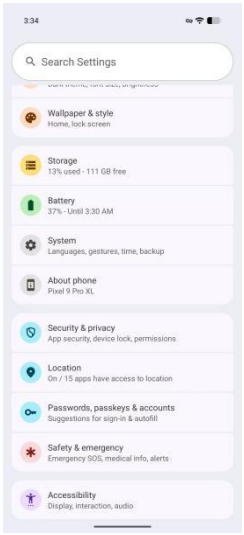


Figure8-10

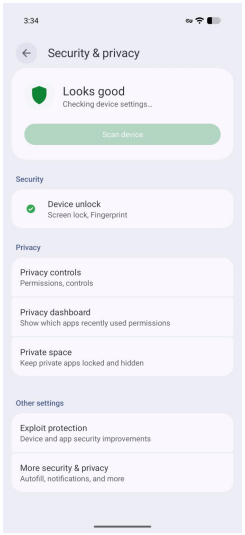


Figure8-11

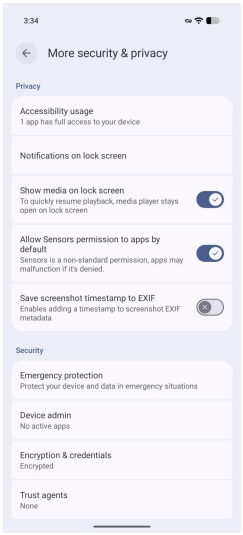


Figure8-12

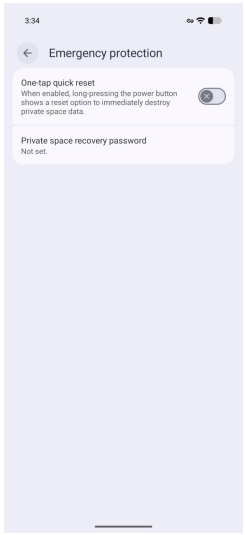


Figure8-13



Figure8-14

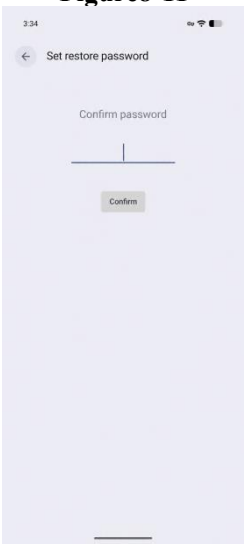


Figure8-15

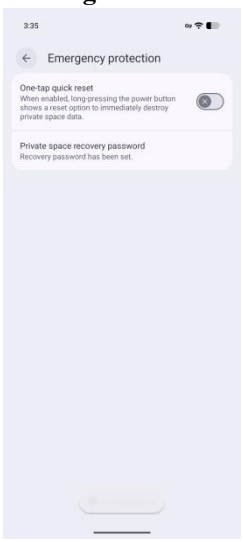


Figure8-16

Helpful Tip: Please ensure this password is completely distinct from your Main Space and Private Space unlock passwords. Note: After a Private Space reset is triggered on the device, you must restart the phone before you can re-create or switch to a Private Space again.

8.3 How to Remotely Lock and Reset

8.3.1 Remote Lock and Tracking

"Remote Location Tracking" provides you with high-precision coordinates of a disconnected device. Coupled with "Lost Mode," you can remotely issue a lock command to prevent unauthorized access to the system while activating location tracking to record the device's movement path in real time, offering critical clues for device recovery.

① Accessing Device Management

As shown in Figure 8-17, open the Device Management app. In the Home Screen Control Center, tap the My Devices item to enter the management list of all linked endpoints under your account.

② Locking the Target Lost Terminal

As shown in Figure 8-18, locate and tap the lost device you wish to manage from the device list (e.g., Pixel 9 Pro XL). The system will attempt to establish a secure remote connection with the device.

③ Enabling Lost Mode Options

Once successfully connected, the interface will display the device's real-time (or last known) geographical location. As shown in Figure 8-19, tap Lost Mode in the function menu below.

④ Lost Mode Initial Configuration

As shown in Figure 8-20, enter the setup page:

Enable Lost Mode: Toggle on the primary switch to prepare the remote device for locking.

Lost Tracking: Simultaneously enable this option. The system will record the entire movement path of the device during the lock period rather than just a single coordinate point.

⑤ Configuring Lock Screen Messages and Deploying Commands

As shown in Figure 8-21, you can further fortify device protection:

Custom Lock Screen Info: Toggle on the Set Lock Screen Message switch. Enter your contact information or return reward details in the text box.

Deploy Command: Once all configurations are verified, tap the blue Enable Lost

Mode button at the bottom.

Track History: Once enabled, you can tap the View link next to Lost Tracking to trace the device's historical movement path.

⑥ Identity Security Check (First-Tier Verification)

As shown in Figure 8-22, to prevent unauthorized operations, the system triggers an identity check. Enter the login password of your VEILORA OS management account in the prompted dialog box and tap OK.

⑦ Target Device Lock Screen Password Verification (Second-Tier Verification)

To ensure the legitimacy and enforcement of the command, the system requires verification of the target device's low-level lock screen password, as shown in Figure 8-23:

Dual-Space Verification: Enter the unlock PIN of the device in the Main Space Lock Screen Password field. If the device has an active Private Space, you must simultaneously enter the corresponding Private Space Lock Screen Password below.

Command Activation: Tap Verify. Upon validation, the remote command will instantly be delivered to the lost terminal, forcing it into a locked state immediately and displaying your pre-set message.

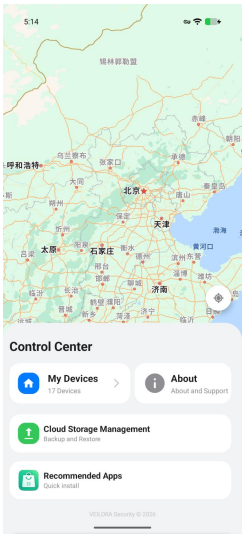


Figure8-17



Figure8-18

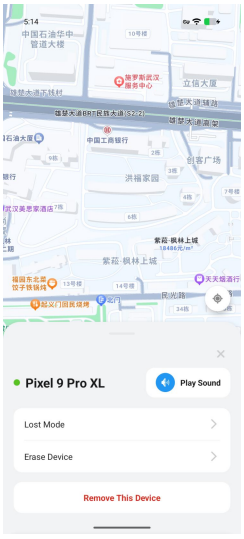


Figure8-19

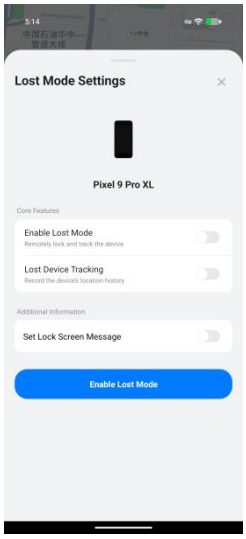


Figure8-20

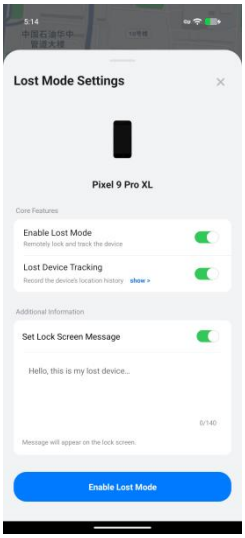


Figure8-21

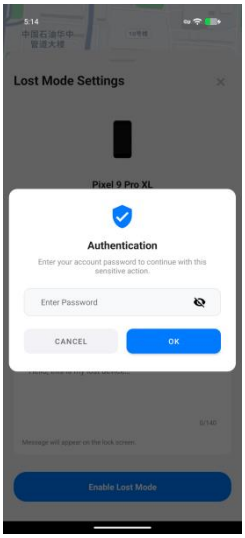


Figure8-22

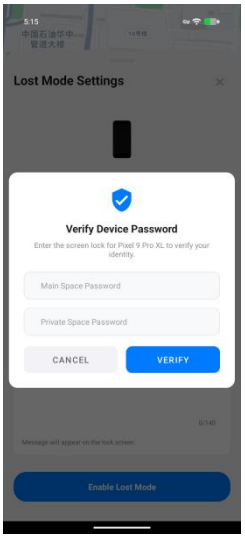


Figure8-23

Operational Tip: Once a remote lock is successfully executed, the device cannot bypass the lockout by any means unless unlocked using your pre-set correct password. To remove the lock after recovering the device, simply enter a new local lock screen password.

8.3.2 Remote Reset

If a lost device is confirmed to be unrecoverable and contains highly sensitive information, this feature can be used to remotely initiate a Private Space reset.The system will forcibly perform a Private Space reset to help reduce the risk of unauthorized access to sensitive data and digital assets.

① Accessing Device Management

As shown in Figure 8-24, open the Device Management app on another trusted VEILORA device. In the Home Screen Control Center, tap My Devices to view the asset list linked to your current account.

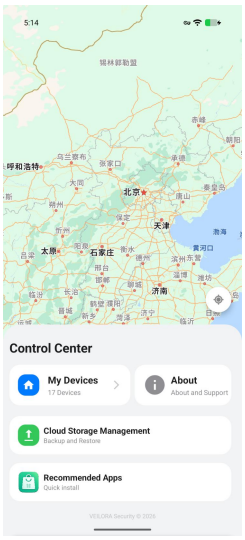


Figure8-24

② Select the Target Device to Reset

As shown in Figure 8-25, precisely select the target device name in the device list to perform a Private Space reset on (e.g.,

Pixel 9 Pro XL). The system will enter the remote real-time monitoring interface for that device.

③ Enabling the Reset Option

As shown in Figure 8-26, locate and tap Erase Device in the operational menu below the device details page. The system will pre-scan the environment and prepare to establish a high-privilege encrypted command channel.

④ Confirming Erase Details and Acknowledging Risks

As shown in Figure 8-27, a critical confirmation dialog box will prompt you, asking "Erase device?". Before proceeding, you must acknowledge the following:

Data Deletion: Once the command is activated, the remote device will immediately execute a physical-level full-disk wipe and return to factory settings. All data will be permanently deleted and cannot be recovered.

Continuous Location Tracking: After erasing, the system will still attempt to retain its final location reporting capabilities. However, because the application environment has been reset, you will not be able to initiate any further reset commands.

Execute Action: Once verified, tap the red Erase text at the bottom.

⑤ Double Verification for Identity and Credentials

To ensure that this highest-privilege command is initiated by the actual owner, the system executes multi-tier identity validation (as shown in Figure 8-28):

First Tier: Enter your VEILORA OS management account password.

Second Tier: Follow the system prompts to verify this device's recovery phrase or lock screen password.

Deploy Command: Once verified, tap OK. The privacy space reset command will immediately deploy through an encrypted tunnel. The moment the remote device connects to any network, it will bypass all states to instantly launch a silent erasure process of the Private Space and full-disk system data.



Figure8-25

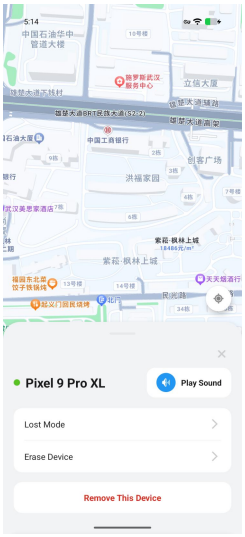


Figure8-26

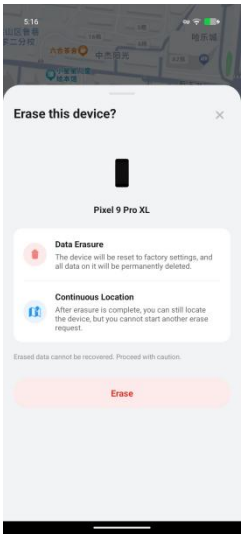


Figure8-27

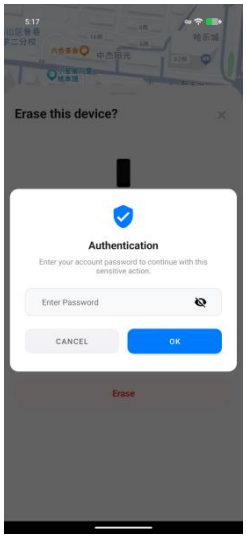


Figure8-28

Security Reminder: Remote reset operations are completely irreversible. Once executed, unsaved data on the device cannot be recovered. We highly recommend utilizing the Cloud Space Management feature during daily use to regularly back up critical data to your WebDAV space, allowing for rapid recovery when migrating to a new device.