Entrust Identity

Mobile App Release Notes

Mobile App release: 25.2.2
April 2025

Document issue: 1
April 2025

This document provides information about the Entrust Identity mobile app, a new generation of the app that combines three legacy apps: the Entrust IdentityGuard Mobile Soft Token app, the Entrust IdentityGuard Mobile Smart Credential app, and the SMS Passcode app. The app works with the Entrust Identity family of products, Entrust Identity as a Service (formerly IntelliTrust), Entrust Identity Enterprise (formerly Entrust IdentityGuard), and Entrust Identity Essentials (formerly SMS Passcode).

The Entrust Identity mobile app resides on a user's mobile device and contains one or more "Identities", which can be Token Identities (instances of the soft token-generating program associated with one or more issuers or "Identity Providers"), Smart Card Identities (encoded information about a user that can include certificates, contact information, fingerprint data, a facial image, and more), or Passcode Identities (which communicate with an Entrust Identity Essentials account) enrolled by an Identity Provider.

The capabilities of these Identities depend on what is configured by an Identity Provider (an organization that uses an Entrust Identity product to issue the Identity to users, for example, a bank or a company). For example, Token Identities can be used for authentication, just like a security code generated by a hardware token. Token Identities can be used to authenticate and to verify transactions by confirming notifications pushed to a user's mobile device. Smart Card Identities can be used to authenticate, to log in to a computer without a password, to verify transactions, and to digitally sign transactions. Passcode Identities can be used for multifactor authentication.

The sections that follow describe features, known issues, platform and operating system requirements, and notes about installing and running the app.

System requirements

Supported mobile device platforms

The 25.2.2 version of the app is supported on the following mobile devices:

- Google® Android™: 11.0 or newer. The Passwordless login to Mac feature requires Android 13.0 or 14.0
- Apple® iPhone and Apple® iPad™: 15.0 or newer. The Passwordless login to Mac feature requires iOS 16.0 or 17.0

Note: Older mobile devices might be able to run older versions of the app if they are still available, however, the older versions will no longer receive updates and are no longer officially supported.

Current version of the app for each device type

The Entrust Identity mobile app uses calendar-based versioning. The releases are numbered like this, **YY.NN.V** where:

- **YY** is the release year,
- **NN** is the release number for that year,
- **V** is the patch version for release,

Every new release of the mobile application replaces all previous versions.

The following table lists the current version of the Entrust Identity mobile app for each device type, and where you can get it.

Device type	App current version	Available from…
Android	25.2.2	Google Play
iPhone, iPad	25.2.2	Apple App Store

Entrust Identity Enterprise requirements

The app requires the following minimum Entrust Identity Enterprise software base, but the newest features may be supported only with current version of Entrust Identity Enterprise (13.0 with latest patch):

- Entrust Identity Enterprise Server 13.0
- Entrust Identity Enterprise Self-Service Module 13.0

Entrust Identity as a Service requirements

This release of the app works with the latest version of Entrust Identity as a Service.

Entrust Identity Essentials requirements

This release of the app works with Entrust Identity Essentials 8.x or later. User accounts must be configured to receive messages through the Entrust Identity mobile app.

Entrust Identity Bluetooth Smart Credential Reader for Windows

The Entrust Identity (IdentityGuard) Bluetooth Smart Credential Reader for Windows, version 3.1.0, is required on user computers to support login to a Windows computer with a Smart Identity.

Entrust Identity Bluetooth Smart Credential Reader for Mac

The Entrust Identity (IdentityGuard) Bluetooth Smart Credential Reader for Mac, version 1.1.0, is required on user computers to support login to a Mac computer with a Smart Identity.

Features of this product

The Entrust Identity mobile app has the following features.

Identities protected by PIN and biometrics

Access to the Identities in the app can be protected by a 4-digit PIN. If an Identity Provider policy specifies that a PIN is required, users must enter the PIN to open the application or continue using it after it goes dormant due to inactivity. The PIN can be enforced by Entrust Identity policy, or you can allow users to turn it on or off as they wish. The amount of time after which the user is required to re-enter their PIN is configurable through the app. If PIN protection is enabled, users can enable biometric PIN alternatives (such as fingerprint recognition or face recognition or other app-supported biometrics), as allowed by device capabilities and Identity Provider policy.

The facial pattern is encrypted through the Advanced Encryption Standard algorithm, using a code of 256 bits (AES256). This algorithm was chosen as an encryption scheme by National Institute of Standards and Technology (NIST) and later was adopted as standard by the Government of the United States.

OATH-compliant time-based OTP generation

The soft token generates a six- or eight-digit security code that can be used one time. The security code changes every 30 seconds. The security code is generated using an algorithm that is compliant with the Initiative for Open Authentication (OATH).

Whether the code is six or eight digits long is configurable through Entrust Identity as a Service or Entrust Identity Enterprise policy. The 30-second time interval is not configurable.

Branding

You can brand the Entrust Identity mobile app with your organization's logo, name, and color.

Multiple Identities

An Identity represents a user's association with an organization that uses an Entrust Identity product for authentication and issues an authenticator to the user. A user's app can manage Identities from your organization and from other organizations that use Entrust Identity products. For example, a user might have Token Identities to access websites or applications for an employer, a bank, and a government self-service website. Users select the appropriate Identity to use for authentication or transaction verification with each Identity Provider. Access to each Identity can be protected with its own PIN and biometric.

Easy download, activation, and management through Entrust Identity user portals

Users can download the app directly from Google Play or the Apple App Store. The Android version can also be distributed to users through your own self-service portal, if desired.

After users have installed the app, they activate Identities through your Entrust Identity product's self-service site. Activation is as simple as scanning a QR code from your self-service website or clicking a link in an email.

After activation, the self-service site also offers Identity management capabilities. For example, users can unlock an Identity and reset its PIN after forgetting it or disable it if they misplace the mobile device with the app installed. Use of self-service reduces calls to your help desk.

Passwordless login to Windows and Mac computers

When configured by the Identity Provider and the mobile device user, this feature allows a user to log in to a computer without entering username and password credentials. Instead, through a Bluetooth connection between the Entrust Identity (formerly IdentityGuard) Bluetooth Smart Credential Reader on the computer and the user’s mobile device, the user’s identity is confirmed by reading the encoded Smart Identity in the

app. The app also supports manual connection and Auto Connect variations of the login. On Windows, the easiest login uses Auto Connect. Users open the app and approach the computer, establishing a Bluetooth connection, then respond to a notification on the app and unlock the computer with biometric authentication or a PIN through the app. On Mac, when the app is open and the computer is active, a Bluetooth connection is established and the Mac prompts the user for a Smart Identity PIN to unlock the computer.

Smart Login to resources protected by Entrust Identity as a Service

Identity Providers that use Entrust Identity as a Service to protect websites and applications can offer their users the Smart Login features. With this feature, users first configure their Smart Identities to log in to a computer. For Windows users, after logging in to the computer with their Smart Identity, they go to your Entrust Identity as a Service website and log in. The app prompts the users to authorize the browser used to reach the website. Next time the user uses that Smart Identity for computer login and opens the authenticated browser to access your Identity as a Service website, they are logged in automatically and can access all protected applications associated with their account without authenticating again. For Mac users, the experience is the same except that Passwordless Login to the Mac with a Smart Identity is optional. They can use the Entrust Identity as a Service Smart Login feature even after logging in to the Mac with traditional user name and password credentials.

Transaction notification

As part of the transaction verification feature, you can optionally enable transaction notifications, which are alerts that indicate to the mobile user that a pending transaction is waiting for them. The alert is accompanied by a ring tone or vibration and appears even if the Entrust Identity mobile application is closed, or the mobile device is dormant.

If you enable transaction verification without transaction notifications, users still receive transaction details, but they do not see a notification alerting their arrival. Users must open the Entrust Identity mobile app to view and confirm the pending transaction.

Transaction verification

Transaction verification is an optional feature available for use with Entrust Identity products. When enabled, users are sent the details of a pending transaction started on your website--a money transfer, for example. Users simply tap Confirm, Cancel, or Suspicious in the app after reviewing the transaction details. "Confirm" generates a confirmation code (an OCRA digital signature of the transaction details) and sends it to the website to complete the transaction.

By having a confirmation notice sent to a secondary device, man-in-the-browser attacks are mitigated.

Action history

If you enable transaction verification, Entrust Identity products keep a history of transactions and their corresponding details for easy browsing.

Available in multiple languages

The app automatically presents the user interface in English, French, German, Japanese, Spanish, Arabic, Danish, Norwegian, and Swedish to match the device's current default language or locale. Some mobile devices allow you to select the language to use in your mobile device settings. If you are using a locale that does not have a translation, English is shown.

Support for queued Token Identity transactions

For organizations that require app users to respond to many transaction verification requests, the app supports holding multiple transactions while waiting for a user response. When this feature is not configured, the default behavior is to have only one active transaction at a time, meaning that a new transaction

overwrites an existing pending transaction. With this feature, the number of transactions that can be lined up and the period of time before they expire are configurable.

Usage of mobile apps on unsecured devices

Identity providers have the option to allow users to run the app on an unsecured device, that is, on an Android device that has been rooted or an iOS device that has been jailbroken. Configuration of this option is done through Token policies in Entrust Identity as a Server or Entrust Identity Enterprise.

Offline transaction verification using a QR code

Users who have mobile devices with no Internet connection can capture transaction details from a QR code displayed on a different device (for example, a bank machine), confirm that they want to proceed, and receive a security code to enter to complete the transaction. The mobile device on which the soft token application resides must have a camera. This feature is configured through Entrust Identity Enterprise Self-Service Module. For more information, see "Enabling automatic activation, transaction verification and security challenges" in the *Entrust Identity Enterprise Self-Service Module Installation and Configuration Guide*.

Logging

The app includes built-in logging capabilities that allow a user to email logs to support.

Reset of Identity Provider account password (Token Identities only)

The app supports resetting user passwords associated with Token Identities managed by Entrust Identity as a Service, including Active Directory passwords associated with Identity as a Service accounts.

New in this release – 25.2.2

No new features added in this release

Fixed:

Error in TOTP registration (IDGM-14160, IDGM-14080, IDGM-14081)

TOTP identities creation was randomly failing due to invalid serial number generation. This issue has been resolved.

(Android) DNS lookup error due to outdated cached IP for a domain on the device (IDGM-14082).

The app was unable to connect to the server until the device refreshed the cached IP. This issue has been resolved.

Please check “**Known issues and limitations**” section for a new behaviour change.

(Android) Random crashes on Android 15 when the app hides the keyboard (IDGM-14061).

The app was causing random crashes on Android 15 devices when hiding the screen keyboard on various screens. This issue has been resolved in this version.

Release history

25.2.1

No new features added in this release

Fixed:

In version 25.2.0 of the Android app, an issue was identified where Android Soft Token PUSH Notifications were not showing when the app was closed (IDGM-14036, IDGM-14034)

> In version 25.2.0, there was an issue that prevented the app from displaying transaction notifications when it was completely closed and running a version lower than Identity Enterprise Self-Service Module Release 13, Patch 623365. However, if the user accessed the app, they could still view the transaction information. This issue has now been resolved.

In the iOS app, an issue was identified where offline transactions were not working when using a long description (IDGM-14053)

The use of long descriptions when processing offline transactions could cause the app to fail in processing them correctly and in completing the extraction of transaction information. This error caused the application to not display transaction information and remain in an unstable state. This issue has now been fixed

25.2.0

New features and enhancements

Policy Synchronization:

Entrust Identity App introduces a policy synchronization feature for online tokens, enabling administrators to update policies and apply them to existing Soft Token Identities. If the app detects changes in the policies a warning icon will appear in the identity, this change may cause new screens to appear when the app is running.

This synchronization is performed during application startup. It requires the device to be connected to the service provider and that the service provider support this feature.

The app distinguishes between two types of updates:

- **Informative Updates:** These updates display a message to the user informing them of changes in the configuration. The user can only accept the update.
- **Action Updates:** These updates require user action, such as changing PIN size. In such cases, the user will be guided through the necessary steps to comply with the policy update. The app will automatically check if the user's existing PIN adheres to the new rules and will prompt an update if necessary. If a user's current PIN doesn't meet the new length requirement, the app will display a warning icon, guiding the user through the process of updating their PIN.

Note: In this version, Entrust Identity app supports this feature for the new **Pin Length** and the existing **Allow Biometric Authentication**.

Pin Length Policy

The 25.2.0 release introduces an updated PIN policy, allowing PINs ranging from 4 to 8 digits for online tokens.

Key Highlights:

- **Automatic PIN Migration:** If a user's existing PIN doesn't meet the new policy, the app will prompt them to update their PIN.
- **Error Handling:** Clear error messages will appear if a user enters the wrong PIN, ensuring a smooth experience.
- **PIN Rules:** The app will make sure your new PIN is secure. It won't let you use simple sequences (3-digit consecutive like 1234) or repeated digits (4-digit sequential like 1111). If you try to enter one of these, the app will ask you to pick a different PIN.

FAQ's:

- **What Happens If You Enter the Wrong PIN:** If you enter the wrong PIN, the app will show an error message and allow you to try again. If you continue to get it wrong, you can keep trying until you enter the correct PIN.
- **Offline Activation of Soft Token:** In the 25.2.0 release, users can activate their soft token offline when IDE/IDaaS is not reachable. During offline activation via QR code, the PIN length will follow the PIN length policy contained in the QR code. For manual input, the PIN length will default to 4 digits, as the app cannot retrieve the updated PIN policy from the server.

New Maximum length rule added for user password change (IDGM-13702):

Since version 5.39 of Entrust Identity as a Service, administrators can define a maximum length for user passwords. The Entrust Identity App includes and evaluates this new rule when users are defining a new password.

Android app background protection (IDGM-13616):

From Android 13 onwards, the application does not display its contents when in the background. This security enhancement prevents the observation of sensitive information when the application is in the background.

Fixed:

In Android, some devices with bold font enabled were not able to see all the digits required to register an offline Soft Token (IDGM-13869, IDGM-13908)

Issue Fixed. Now, users can see all digits when using bold fonts.

In iOS17, wire transfers using offline Soft Token authentication were not working with Identity Enterprise. (IDGM-13725)

Issue Fixed. Users were not able to complete the process as the buttons appeared disabled.

Some users were not able to receive push notifications and transactions in some identities (IDGM-13684)

After a change of the notification token by Apple, in some situations, some identities could fail to correctly register this token on the server and cause this error. This issue has been fixed.

An Error message appeared in 24.4.0 when trying to register a TOTP. (IDGM-13655)

Issue Fixed. A generic message was displayed when the user tried to register a new TOTP using a name that was already registered in the app. The message has been changed to provide more accurate information to the user.

Updated:

Onfido SDKs have been updated in this version (IDGM-13668)

- Users who updated to this version must use flows compatible with these versions:
    - iOS SDK version has been updated to 32.1.1.
    - Android SDK version has been updated to 22.2.1.

25.1.1

No new features added in this release

Fixed:

In Entrust Identity App version 25.1.0, offline soft token activation fails when the provider URL is not empty and unreachable, and the internet connection is available. (IDGM-13683)

The fix has been implemented to restore the offline activation fallback when the provider URL is unreachable.

In Entrust Identity App version 25.1.0, offline soft token activation fails when the provided QR code contains an empty provider URL. (IDGM-13683)

A fix has been implemented to support this scenario.

25.1.0

New features and enhancements

Soft Token Verification Enhanced with Face Biometric Authentication

In this release, we have enhanced the existing Soft Token Activation process by integrating Face Biometric Authentication as an additional layer of security. This enhancement further strengthens the identity verification process, ensuring a more secure activation experience.

Key Highlights:

- **Face Biometric Authentication Integration:** Starting from Identity as a Service 5.38, during the activation of the soft token, if the policy requires it, users will be required to complete face recognition via Onfido platform. This ensures that only authorized users can register the soft token on their devices. After the soft token is activated, face biometric verification will not be required during future logins or transactions.
- **Enhanced Security:** Integrating face biometric authentication with the soft token activation process provides a higher level of security, preventing unauthorized users from registering a soft token.
- **Seamless User Experience:** Users will experience a streamlined process for activating the soft token and performing the biometric verification directly from their mobile device, eliminating the need for physical hardware tokens.

EULA Update for Maps Instances and Face Biometric Features

This release includes an updated End-User License Agreement (EULA) to accommodate the integration of Maps instances and Face Biometric functionalities. The updated EULA must be accepted by all users, both for new installations and upon updating to the latest app version.

Key Highlights:

- **New EULA Acceptance:** The new EULA must be accepted by all users.
- **New Installations:** The updated EULA will be presented and must be accepted during the first-time installation of the app.
- **App Updates:** Existing users will be prompted to accept the new EULA upon updating to the latest app version.
- **Feature Updates:** The updated EULA includes provisions related to the newly integrated Maps instances and Face Biometric features.

Fixed:

The Report button fails to mark a manual/offline transfer as suspicious, causing the transaction to fail. (IDGM-13590)

> The Report button functionality has been updated to work as the Suspicious button in the new app version to prevent transaction failure.

The app fails to properly manage expiry notifications when the user is registered in two environments with the same User ID, causing one notification to disappear. (IDGM-13274)

> Updated the app to fix this issue, ensuring that expiry notifications from both environments are handled correctly.

Users were able to successfully migrate soft tokens using Apple's quick start to transfer Soft Token identities to other device from the same owner (IDGM-12963)

> After implementing the fix, the migration of new or edited soft tokens using that tool is no longer possible.

24.4.0

Face Biometric Identity

Face Biometric Identity has been introduced in this release. The face biometrics are stored encrypted & hashed within the Identity App. Face Biometric Identity allows users to securely register, authenticate, delete, and manage their identity within the app, enhancing user verification and transaction handling.

Key Highlights:

- **Registration Flow:** Users provision their identity using a QR code and complete face recognition via Onfido platform. Details must be confirmed before proceeding.
- **Step-up Flow:** Push notifications alert users about authentication processes. Users can confirm, cancel, or mark actions as suspicious.
- **Delete Flow:** Users can swipe to delete their face identity with confirmation. Handles no internet connection and unreachable provider scenarios.
- **Update Flow:** Manages expired identities with notifications and update processes. Allows re-registration if an identity expires.
- **Transaction History:** Users can access their action history with or without OS-level security. Security prompts ensure safe access to sensitive information.

New Token Policy to Disable Biometrics in the Identity App

This feature allows the app to apply the new policy added on the Identity Providers:

- Entrust Identity as a Service will support this feature since 5.37 version
- Entrust Identity Enterprise will support this feature since the patch Server/Self-Service 13 Patch 623359 / 623360

If the policy is activated, the application will not allow the user to use phone local biometrics to protect the new Soft Token identities created.

Key Highlights:

- **Compliance with Regulations:** The policy aligns with the Central Bank of Egypt's new banking regulations, which mandate the disabling of biometrics for token access.
- **PIN-Only Access:** Customers will only be able to use a PIN to unlock their tokens, ensuring secure access without biometric authentication.
- **Policy Implementation:** A new policy category will be introduced to enforce the restriction on biometric unlocks, maintaining compliance and security for mobile/internet banking.

Fixed:

The Users were facing some UX issues with "Reduce Motion" setting or battery saver enabled. (IDGM-13008)

Users were facing missing browser prompts during Smart Identity authentication, can't delete registered computers without uninstalling, and bottom sheets don't display with "Reduce Motion”, or battery saver enabled. This issue has been fixed.

Improvements:

Upgrade Mobile Smart Credential from SCP 02 to SCP 03. (IDGM-9615)

The Mobile Smart Credential has transitioned from SCP 02, which used 2-key TripleDES, to SCP 03, utilizing AES for enhanced security in accordance with NIST SP800-131A. The updated app version supports SCP 03 while ensuring compatibility with existing Secure Credentials during activation and updates.

Important!

The minimum Identity Enterprise required version to support this protocol is IdentityGuard 12 patch 86284, released in November 2018

In Passwordless login to Windows Feature, add detection of Device Agent Version and management of Non-Authenticated Bluetooth Channel. (IDGM-12941, IDGM-12945)

Using Device Agent version 4.0.0 or newer, the app can unsubscribe from the non-authenticated channel when not needed to enhance Bluetooth stability. It remains compatible with older devices and ensures smooth reconnections without errors during disconnection.

24.3.0

Password Expiry Notification

In the latest version of the Mobile Identity App, we're introducing a new type of notification. Users will receive a push notification when their account password is about to expire. This notification will appear in the main app as a warning and will allow users to change their password directly from the app. The feature can be enabled or disabled by the Entrust Identity as a Service integrator, who can also configure the frequency of notifications.

Key Highlights:

- **Warning for Expiring Passwords:** Users will receive a push notification warning them when their account password is close to expiration. The app will display the remaining time until expiry.
- **Password Change Option:** Users can change their password directly from the app after receiving the notification, thereby extending the expiration period.

Note: This feature is exclusively available for Entrust Identity as a Service and for Token identities registered for online transactions.

Fixed:

The "Available Computers" screen showed as blank/white upon connection failure instead of maintaining the list of found computers. (IDGM-12468)

Modified app behavior to retain the "Available Computers" screen with the list of found computers upon connection failure, allowing users to retry connections seamlessly.

App did not update to reflect Bluetooth on/off changes at OS level. (IDGM-12515)

Updated app to promptly respond to Bluetooth status changes, enabling seamless computer addition after Bluetooth activation without repeated prompts.

Input text fields makes a weird animation when entering values in it (IDGM-12655)

Resolved

The QR scan permission screen briefly displays "Allow" instead of "OS Settings" after camera permission is removed at the OS level. (IDGM-11652)

Modified the app to consistently display "OS Settings" on the QR scan permission screen immediately upon opening, regardless of prior camera permission status changes at the OS level.

App freezes when rapidly toggling the computer list filters on the computer search screen. (IDGM-12309)

> Implemented stability improvements to prevent app freezing when quickly toggling computer filters, ensuring smooth functionality during filter adjustments.

The Soft Token stopped working after a recent update. Despite attempts, it fails to authenticate. (IDGM-12578)

> Soft Token could become out of sync causing a mismatch between the token seed in Entrust Identity as a Service and the mobile app when a new device token was received due a race condition. It was rarely reproducible. Ensured synchronization between the app and Entrust Identity as a Service token seeds to resolve the issue.

Mobile Smart Credential authentication fails if there are more than one pending challenge in the "Actions" section of the Mobile Identity app. New challenges throw the error "Something went wrong: Failed to fetch pending challenge information." (IDGM-12674)

> Updated the Mobile Identity app to handle multiple pending challenges for Smart Credentials correctly. Ensured that all pending challenges associated with the same token ID are managed and resolved without errors during authentication processes.

24.2.0

Elliptic Curve Cryptography (ECC) Smart Identity support:

In this version of the Mobile Identity App, we're introducing support for Elliptic Curve Cryptography (ECC) keys on smart identities. Specifically, the app now accommodates the NIST Curve P-256, enhancing compatibility and security, particularly for Identity Providers that mandate this standard on Android and iOS devices.

Key Highlights:

- **Expanded Compatibility:** Users can now seamlessly interact with Identity Providers that require ECC keys, ensuring smooth operations on both Android and iOS devices.
- **Enhanced Security:** ECC keys, particularly the NIST Curve P-256, offer robust cryptographic security, fortifying the protection of smart identities within the app.

Hardware storage Smart Identity keys indicator:

Starting from this version, the Mobile Identity App has been upgraded to incorporate the latest Mobile Smart Credentials SDK version 4.8.0. This update introduces significant enhancements, including the capability to securely store Smart Identity keys on supported hardware storages provided by Android and iOS devices.

Key Highlights:

1. **Enhanced Security:** The Mobile Identity App now supports the storage of Smart Identity keys on secure hardware storages available on both Android and iOS devices. This ensures an additional layer of protection for sensitive data.
2. **Improved User Experience:** Users will notice a new icon displayed on the Smart Identity details screen, indicating the storage location of the device-generated keys. This provides transparency and reassurance regarding the security measures implemented.

3. **Additional Information Access:** For further details regarding the storage location of the keys, users can easily access more information through the "Learn more..." option. This option directs users to a dedicated web page offering comprehensive guidance on the topic.

Platform-Specific Enhancements:

- **iOS:** Added support for Secure Enclave, ensuring secure storage of Smart Identity keys on compatible iOS devices.
- **Android:** Introduced support for StrongBox Keymaster and Trusted Execution Environment (TEE) storages, further enhancing the security of Smart Identity keys on Android devices.

Important!

The decision of the generation place resides on the device, the OS and the type of keys requested from server. Not all devices and OS support all the storage and all keys on their storage. Please, check with the manufacturer for more details. App will try to generate the keys in the securest place possible.

The generation of keys in a secure storage may require extra time and may affect the activation time of the Smart Identity. The speed will depend on the device's specifications.

Latest Entrust Identity as a Service version also supports adding some restrictions on generation as requirement. Please check Entrust Identity as a Service documentation to get more details.

For troubleshooting purposes, app added an option to adjust log levels for the app, SDK, and JS SDK in the App settings. (IDGM-12198, IDGM-12187)

Implemented a feature allowing users to change log levels by long-clicking in the App settings under Build field. Users can now set log levels for the app and SDK to Debug or Info, and for the JS SDK to Debug, Info, or Off. After a value change, an app restart is required.

Fixed:

Soft tokens could be removed if the user closes the app when the associated file it is being saved (IDGM-12451)

This issue has been fixed and the previous saved version will be restored if that occurs.

Improved user actions on the Passwordless screen (IDGM-11844)

Users can now seamlessly add a new computer, prompting disconnection from the current one, and switch to another saved computer, automatically terminating the current connection upon selection.

The Details screen in the transaction history did not dynamically update its color scheme based on changes made by the admin in the admin portal. Previously, the color was fixed and not updated dynamically. (IDGM-11388)

Added dynamic color functionality to transaction history Details screen. Now, changes made to logo, app color, or theme in admin portal are instantly reflected in the app, ensuring consistency and immediate updates across platforms.

(iOS) After prolonged background periods, app is not able to perform Windows login. (IDGM-12284)

The current app version can recover the connection when the OS makes the webview stops running. This issue has been solved.

(Android) Bluetooth disconnected when removing the Bluetooth headset from the computer. (IDGM-12291)

In some situations, app was restarting when disconnecting Bluetooth devices. This issue has been solved.

Users see unexpected screens on Windows devices when login notification is not processed and the login process is not cancelled. (IDGM-12192)

This issue is due to a Windows behavior when the login process is not cancelled. The new app version uses cancel the process after some time if login is not processed.

(iOS) The app autoconnects when moved to background after a manual disconnection with auto-connect setting enabled. (IDGM-12180)

This issue has been fixed.

The "Auto Connected to.." toast message was incorrectly displayed when manually reconnecting, despite auto-connect settings being disabled. (IDGM-12186, IDGM-12217)

The issue has been resolved.

(iOS) In some situations, the App was repeatedly displaying a toast after a connection completed. (IDGM-12185)

The app has been modified to only display the message only once for each connection, eliminating redundant notifications.

(iOS) App experienced unexpected Bluetooth disconnects, notably during tasks like making calls or using Outlook. (IDGM-12208)

Disconnections were due to idle GATT sessions. We've added a manual retry in the iOS app to reconnect. Also, it is enhanced to prevent Windows Entrust Bluetooth reader product from removing smart cards, avoiding random disconnections.

(iOS) App prompts twice for PIN entry. (IDGM-12173)

Multiple login notifications were displayed in the app when a previous login process was not completed, and the user starts a new process. This issue has been solved.

(Android) Entrust Identity was not handling non-acknowledged Windows login requests properly, leading to login failures when users returned to their computer after walking away with their iPhone. (IDGM-12165)

The logic adjusted to update the disconnect status only in cases of manual disconnection, excluding rapid auto-reconnect scenarios.

(iOS) Entrust Identity app hangs in a connecting state when disconnecting and reconnecting multiple times. (IDGM-12228)

This issue has been solved.

(iOS) Users encountered a misleading bottom sheet indicating Bluetooth activation despite Bluetooth being already auto-connected. (IDGM-12224)

Fixed the issue by moving Bluetooth status checks to occur after central manager initialization, ensuring accurate bottom sheet display.

(iOS) The Bluetooth connection drops when moving out and back into Bluetooth range without taking action on the login popup. (IDGM-12218)

This fix includes improvements to the app's auto-connect feature, ensuring a stable Bluetooth connection even when moving in and out of Bluetooth range without immediate interaction with the login popup.

(Android) App failed to detect disabled Bluetooth, causing infinite loading when connecting without Bluetooth enabled. (IDGM-12230)

Added bottom sheet notification to alert users of disabled Bluetooth when attempting to connect.

(Android) Auto-connect is disabled when the app and computer are left idle for an extended period, and the computer enters sleep mode. (IDGM-12242)

App incorrectly disabled Bluetooth when computer slept after long idle. Adjusted to maintain auto-connect during idle and sleep.

(Android) Entrust Identity app loses connection with Windows Bluetooth Reader immediately after establishing the connection. (IDGM-11914)

Fixed by ensuring Android app properly handles update indications from Windows BTR, preventing immediate disconnections post-connection.

(Android) Auto-connect setting in bad state. (IDGM-12170)

In some situations, auto-connect setting was modified in the app without user interaction. This issue has been solved.

23.9.0

New features and enhancements

Enhancements to process for configuring passwordless login to a computer with a Smart Identity (IDGM-11543)

New screens help guide users through the process of pairing a Smart Identity for the purposes of passwordless login to a computer.

There are significant prerequisites for pairing a Smart Identity with a computer, especially with a Mac. The app’s enhanced pairing flow provides some of this information, but previous installation of the Entrust Bluetooth Smart Credential Reader (Windows or Mac version) is essential. For details about prerequisites and configuring Passwordless computer login, refer to the document associated with your Entrust server product:

- Entrust Identity as a Service Administrator Help, or
- Entrust Identity Enterprise Smart Credentials Guide

The information on the app’s pairing flow screens is further supported by the app help, where this feature is documented in the following help topics in the Smart Identities section:

- Activate a Smart Identity
- Passwordless login to a Windows computer

Support for new mobile device OS versions (IDGM-11545, IDGM-11546)

The Entrust Identity app now supports devices running iOS 17 and Android 14.

Enhanced computer searching capability (IDGM-11543)

There were improvements to the way the app searches for supported computers.

(Mac) Bluetooth pairing stability and reliability improvements (IDGM-10460)

The app has been enhanced to improve the stability and reliability of the Bluetooth connection between Mac computers and paired Smart Identities in the app.

(Windows) Bluetooth pairing stability and reliability improvements (IDGM-9281)

The app has been enhanced to improve the stability and reliability of the Bluetooth connection between Windows computers and paired Smart Identities in the app.

Bluetooth reader support on Windows 11 (IDGM-10869)

The Entrust Identity app is now supported with the Entrust Identity Bluetooth Smart Credential Reader when it is running on computers running the Windows 11 operating system.

(Android) Allow app to connect to Bluetooth Reader for Windows using BLE (IDGM-11023)

The Entrust Identity app for Android can connect to a Windows computer using Bluetooth Low Energy (BLE).

23.6.1

New features and enhancements

Support for Smart Card Identity login to Mac computers (IDGM-10620)

The release of the 23.6.1 app coincides with the release of a new version of the Entrust Identity Bluetooth Smart Credential Reader for Mac (or BTR for Mac) - version 1.0.3. This software allows a Macintosh computer with macOS 12 (Monterey) or 13 (Ventura) to read the encoded Smart Card Identity from the Entrust Identity mobile app and prompt the user to log in by entering the Identity PIN instead of user name and password credentials.

For information about installing and working with the BTR for Mac 1.0.3, refer to the following documents available on Entrust TrustedCare:

- Entrust Identity Bluetooth Smart Credential Reader for Mac Release Notes
- Entrust Identity as a Service Administrator Help
- Entrust Identity Enterprise Smart Credentials Guide

Support for Smart Login to Entrust Identity as a Service from Mac computers (IDGM-10459)

A user who has paired a Smart Card Identity and a Mac computer for passwordless login can also take advantage of the Smart Login feature, which reduces the number of times the user is asked to authenticate to Entrust Identity as a Service and the resources that it protects. For details about configuring Smart Login to Entrust Identity as a Service, refer to the Entrust Identity as a Service Administrator Help.

Improved flow for pairing a Smart Card Identity with a computer (IDGM-10902)

New screens help guide users through the process of pairing a Smart Card Identity for the purposes of passwordless login and Smart Login to Entrust Identity as a Service.

Important!

For Mac users, a Bluetooth connection must be established between the Mac computer and the user's mobile device prior to attempting the pairing with a Smart Card Identity. The connection must be initiated from the Mac and requires the user logged in to the Mac to have administrator privileges. The app's pairing screens provide information about this and other prerequisites, but Identity Providers and users should learn about and complete prerequisite tasks before attempting an Identity/Mac pairing. In addition to the server product documentation, refer to the app help section **Smart Cards > Mac passwordless computer login**.

Features of the **Searching for computers** screen include

- Tap the MacOS or Windows filter buttons to show only computers of the selected type.
- Toggle between **tile view** and **grid view** buttons to change the display of the found computers. If a user returns to this screen later, the previously selected view persists.
- Use the **Search** bar to search for a specific computer.
- If no computers are found within 30 seconds, swipe down on the screen to search again.
- Tap **Can't find my computer** to open a troubleshooting page in help for advice on finding the computer.

Note about Supported Computers.

The Android version of the Entrust Identity mobile app cannot connect with the Entrust Bluetooth Reader for Windows over Bluetooth Low Energy (BLE). Some Android devices are not able to find Windows computers as Classic Bluetooth. In this case, a computer is listed as Not Supported.

Improved guidance for pairing a Smart Card Identity with a computer (IDGM-11052)

The new pairing flow is included as part of the activation flow for a new Smart Card Identity. If a user chooses not to pair a computer when activating an Identity, they can initiate it later by tapping the **Passwordless** icon in the app.

There are significant prerequisites for pairing a Smart Card Identity with a computer, especially with a Mac. The app's new pairing flow provides some of this information, but previous installation of the Entrust Bluetooth Smart Credential Reader (Windows or Mac version) is essential. For details about prerequisites and configuring Passwordless computer login, refer to the document associated with your Entrust server product:

- Entrust Identity as a Service Administrator Help, or
- Entrust Identity Enterprise Smart Credentials Guide

The information on the app's pairing flow screens is further supported by the app help, where this feature is documented in the following help topics in the Smart Cards section:

- Activate a Smart Card Identity
- Passwordless login to a Windows computer
- Passwordless login to a Mac computer

Time zone added to Android logs (IDGM-11206)

Previously, the Android app logs showed the user's local time but no time zone. This made it difficult for troubleshooting when comparing the app logs with server logs. The new app log format now includes the user's time zone to address this difficulty.

Identity configuration information is updated upon launch of the app (IDGM-11022)

If an Identity Provider has updated the server configuration (logo, color scheme and other branding), this configuration is updated in associated Token and Smart Card identities as a background task when the app is launched. Previously, users had to select the Edit icon (pencil) for the Identity to perform this update. They can still use the Edit feature to edit the Identity name and update certificates, when required.

Improvements to permissions requests (IDGM-10653)

Pairing a Smart Card Identity with a computer requires that a user grant a permission *for the Identity app* in the mobile device settings. For iOS devices, the **Bluetooth** permission is required. For Android OS 12 and newer, the required permission is **Nearby devices**. For Android OS 11 or older, the required permission is **Location**. The app informs users why the permission is required and requests that users grant the permission at key points in the configuration of features that require it (including the computer pairing flow that follows Smart Card Identity activation). The user only needs to tap **Allow** to send the permission request to the mobile

device OS. If the user has denied the permission once on iOS or twice on Android, the app button changes to **Open OS settings**. The computer pairing flow cannot be completed until the appropriate permission is granted.

Fixed

App blocked after receiving a transaction when there were many items in transaction history (IDGM-11643)

If the app was opened from a notification and an Identity had a large number of transactions in the Transaction History, the app became unresponsive. This issue has been resolved.

(iOS) App closes unexpectedly after activating Smart Card Identity (IDGM-11219, IDGM-11187)

After activating a Smart Card Identity, the app presents the **Smart Card Identity Ready** screen on which a user can create a pairing with a computer to enable passwordless login. In rare cases, if the user taps **Skip** or **Pair computer** on this screen, the app closes unexpectedly. Upon restarting the app, the Smart Card Identity was seen to be activated successfully and listed on the Identities screen. The user could then pair the identity with the computer by tapping the Passwordless icon  .

Wrong Smart Card Identity is selected when using Auto Connect (IDGM-11611)

When a user had more than one Smart Card Identity paired with a computer, the Auto Connect feature continued to auto connect with the first Identity that had used the feature even after Auto Connect had been turned off for the first identity and turned on for the second. This issue has been resolved.

Random disconnections with Bluetooth Reader for Windows and iOS devices (IDGM-11542)

Due to a thread prioritization issue, the connection was experiencing random disconnections. These errors have been fixed in the current release.

Two iOS devices were auto-connecting to a computer at the same time (IDGM-11269)

The app allowed two iOS devices to appear as connected with the auto-connect feature. Only the first one to perform the process was connected, but the user experience was wrong. This has been fixed in this release.

After users received a pairing error and restarted the app, the computer was saved (IDGM-10858)

Due to an error in the persistence of found iOS devices, devices were being persisted incorrectly after a connection error. This issue has been resolved.

Improved stability of connection between mobile device and computer (IDGM-11587)

The iOS version of the app sometimes did not connect to the paired Windows computer when moving within Bluetooth range. This issue has been resolved.

Changed

Support for Entrust Facial Recognition is discontinued (DGM-11172)

The option to enable facial recognition biometrics through the **Identity Settings > Biometrics > Entrust Facial Recognition** option (and which required a license from the Identity Provider) has been removed. From app version 23.6.1 onwards, facial recognition is supported only on mobile devices that have their own facial recognition capability.

23.4.0

Fixed

App incorrectly detected support for facial recognition and fingerprint recognition (IDGM-11188, IDGM-11197)

Release 23.1.0 of the Entrust Identity mobile app displayed setup instructions for some biometric configuration not supported by the device. This issue has been resolved.

In China, users of App version 23.1.1 could not activate Token Identities online (IDGM-11223)

This issue has been resolved.

Smart Card Identity expiration dates did not consider leap years (IDGM-11203)

The details page for a Smart Card Identity reported a slightly inaccurate expiration date for encoded certificates because it did not consider the extra day in leap years. This issue has been resolved.

Changed

Upcoming change: Support for Entrust Facial Recognition to be discontinued

In an upcoming release of the app, the option to enable facial recognition biometrics through the **Identity Settings > Biometrics > Entrust Facial Recognition** option will be removed. Facial recognition will no longer be supported on mobile devices that do not have app-supported facial recognition through the device's own biometrics settings.

23.1.1

Fixed

App mistakenly prompted users to unlock Soft Tokens that are not PIN-protected (IDGM-11209)

Version 23.1.0 of the Identity Mobile app, after being restarted, mistakenly prompted users to unlock Soft Tokens that were not protected by PIN. This issue has been resolved.

23.1.0

New features and enhancements

Delete an Identity with a swipe action (IDGM-10848)

This version of the app offers a new way to delete an Identity. On the Identities screen, swipe left-to-right or right-to-left, depending on the app's language setting. Tap the trash icon that appears, then confirm the deletion. Alternatively, users can delete an Identity using the Actions list on the Identity's Details page.

(iOS) Improved Bluetooth connection stability during the auto-connect process (IDGM-11026)

This version of the app reduces connection fluctuation to improve the Bluetooth connection stability between the iOS device and computer during the auto-connect process.

(iOS) Security improvement: App details hidden when app is in background (IDGM-10770)

When this version of the app is sent to the background, any previously visible details and data on the app screen are automatically hidden by a security screen. If the mobile app times out and auto-lock is triggered, user PIN or biometric login is required to pass the security screen and access the app.

Changed

No failure reason was specified when a user attempted to create a weak password (IDGM-9838)

Entrust Identity as a Service allows administrators to configure minimum password strength requirements. This version of the app delivers error messages with improved accuracy and precision should a user attempt to create a password that does not meet the minimum requirements or strength level configured by their administrator. This version of the app also improves clarity regarding password requirements.

Fixed

(Android) Identities remained unlocked when app was closed and restarted (IDGM-11198)

If connected to a paired computer over Bluetooth, when a user closed the app and reopened it before the Auto-Lock period had expired, Smart Card and Soft Token Identities that were unlocked when the app was closed remained unlocked and ready for use. This issue has been resolved.

(iOS) Identities could not be edited on some devices running iOS 16.x (IDGM-11024)

On some iOS devices, when users attempted to edit an Identity (for example, change an Identity name) and their keyboard was displayed, their device screen went blank when scrolling up to access the **Save** button. This issue has been resolved.

(iOS) App occasionally crashed when activating Smart Credentials through email (IDGM-11004)

Previously, when Smart Credential activation was encrypted and required a user-entered password, Smart Credential activation through email was unsuccessful and would cause the app to crash. This issue has been resolved.

(Bluetooth Smart Credential Reader for Windows) Autoconnect failed when the app was forced closed and relaunched (IDGM-11018)

When using Entrust Identity Bluetooth Smart Credential for Windows with Android or iOS devices, Autoconnect occasionally failed when the mobile app was forced closed and relaunched. This issue has been resolved.

(Android) Error initiating Smart Credential library (IDGM-11056)

Previously, the app closed unexpectedly upon launch on some devices running Android 12 or newer. This issue has been resolved.

22.11.0

New features and enhancements

Enhanced protection against attacks (IDGM-9248)

This version of the app features Runtime Application Self-Protection (RASP) improvements that secure internal data and intellectual property rights and add greater security against a range of attacks.

Improved the Smart Card Identity pairing process (IDGM-9248)

Added user guidance and optimized the user flow to improve the process of pairing a computer and a Smart Card Identity.

Strengthened minimum TLS requirements (IDGM-9415)

The Entrust Identity mobile app has been updated to strengthen the minimum TLS requirements that a server must meet for the app to connect to it when making HTTP requests. The minimum TLS requirements are as follows:

- The server certificate must be signed with either an RSA key of at least 2048 bits, or an ECC key of at least 256 bits.
- The certificate must use SHA-2 with a digest length, sometimes called a fingerprint, of at least 256 bits (that is, SHA-256 or greater).
- The connection must use TLS protocol version 1.2 or later.
- Data must be exchanged using either the AES-128 or the AES-256 symmetric cipher.
- The link must support perfect forward secrecy (PFS) through ECDHE key exchange.

See also the following note.

Important information for organizations using Entrust Identity Enterprise

Entrust has enhanced the Transport Layer Security (TLS) in version 22.11.0 of the Entrust Identity mobile app (Android and iOS versions). Organizations that use Entrust Identity Enterprise are advised to make corresponding TLS enhancements to their Entrust Identity Enterprise installations, if they have not already done so, to continue to work with the 22.11.0 release of the app and future versions. If you have installed recent Entrust Identity Enterprise patches (Release 13, Server Patch 315066 or newer, SSM Patch 315067 or newer), you might have already made the required updates.

Information about these changes was sent to Entrust Identity Enterprise customers by email in June 2022. This information has also been provided in the release notes for Entrust Identity Enterprise and Self-Service Module since December 2021, however, Entrust recommends that you verify your installation against the advice as described in “Recommended: Manually install new ciphers” in the current patch release notes for the following products:
- Entrust Identity Enterprise 13.0
- Entrust Identity Enterprise Self-Service Module 13.0

Changed

(Android) Supported version updated

Android operating system 9.0 or newer is required to support the latest version of the app.

Fixed

Push notification was not shown and could not be actioned (IDGM-10821)

In some situations, the app did not prompt for credentials to unlock an Identity and the user was not able to access the transaction until the Identity was unlocked. This issue has been resolved.

(iOS only) Bluetooth connection was not established to perform computer unlock (IDGM-10603)

This issue has been resolved. Smart Credential Identities now connect to the Entrust Identity Smart Credential Bluetooth Reader installed on a paired computer when the auto-connect setting is enabled and the Identity mobile app is within Bluetooth range.

(iOS only) Bluetooth connection was disconnecting randomly (IDGM-10647)

This issue has been resolved. The connection with the BTR is now stable.

Bluetooth discovery did not find all devices to pair (IDGM-10893)

The time used to discover Bluetooth devices near the app was increased from 5 to 30 seconds. This issue has been resolved.

Provider's color is not consistently updated (IDGM-10807)

This issue has been resolved. The Identity Provider's custom color was not consistently updated on the app screens.

Unresponsive back arrow displayed on SMS Passcode Identity creation (IDGM-10819)

This issue has been resolved.

22.9.0

New features and enhancements

Support for mutual authentication challenges for soft token transactions (IDGM-10536)

Supported only with Entrust Identity as a Service

When confirming a transaction with a Soft Token Identity, users can be prompted with a mutual authentication challenge. The device issuing the transaction displays a single value as the correct answer to the challenge. To complete the transaction verification, the user must enter that same value in the mobile app or select it from a choice of values shown in the app. Use of a single value or multiple values is configured in the Entrust Identity as a Service "Mutual Challenge Size" setting (Policies > Authenticators > Entrust Soft Token). This feature combats multi-factor authentication fatigue, in which an attacker sends many transaction notifications hoping one is confirmed. The extra challenge prevents the user from confirming the attacker's transaction. This Entrust Identity as a Service feature is not enabled by default.

Improved handling of notifications permission (IDGM-10624)

A new permission-related item appears in the app's settings if notifications are turned off. The text advises users to turn on notifications for the app and provides a link to the mobile device settings.

Improved handling of camera permission (IDGM-10664)

New messages describe when camera permission is required and for what purposes.

Support for activating TOTP tokens (IDGM-8991)

The SDK now supports parsing and activating generic TOTP tokens according to Google's KeyURI format.

Changed

Improved pairing of computers with Android and iOS devices (IDGM-9766)

Previously, Android devices needed to be paired with computers through the device operating system before they could be paired through the app for smart credential computer login. Now the pairing can be complete just through the Identity mobile app.

Fixed

Issues with Bluetooth pairing of Mac computer and Android Identity mobile app (IDGM-10541, IDGM-10551, IDGM-10559)

Various issue of Mac/Android pairing have been revolved including pairing was not retained and could not be re-established, Bluetooth connection was dropped when using the app switcher or sending the app to the Home page, and missing Mac prompt to connect the inserted smart card with the current user.

Correction to Japanese localization (IDGM-10758)

An incorrect word was used to describe an action. This has been corrected.

(iOS) Inconsistent behavior in Action History (IDGM-10709)

After confirming an expired transaction, the Action History displayed the transaction as "Confirmed" instead of "Error". This issue has been resolved.

Identity mobile app shows 9-digit Italian phone numbers as invalid (IDGM-10820)

Existing 9-digit Italian phone numbers were not being validated. This is now resolved.

22.6.1

Changed

Migration of soft tokens from legacy app no longer supported (IDGM-10290)

In previous releases of the Entrust Identity mobile app, Token Identities created in the legacy Entrust IdentityGuard Mobile Soft Token were retained (along with their settings and action history) when users installed the Entrust Identity mobile app. This migration of Token Identities is no longer supported from this release onwards. Users must create new Token Identities in the new app.

Fixed

(Android and iOS) First code generated by soft tokens not accepted (IDGM-10568)

For some users, the fist code generated by their soft tokens were not being accepted. Subsequent codes were accepted. This issue has been resolved.

(iOS) Identity mobile app not showing confirmation button for push until restarted (IDGM-10638)

In some cases, iOS users were intermittently unable to access the Identity mobile app login screen to unlock their Identity and open a transaction without restarting their device. This issue has been resolved.

22.4.0

New features and enhancements

Entrust Identity Essentials Passcode Identities support message decryption policy (IDGM-10011)

Prior to app release 22.4.0, when a user received a notification for a Passcode Identity, the notification stated only that a new message had arrived, and the user had to tap the notification to open the app and view the message. Now, if your Entrust Identity Essentials Identity Provider has configured the Message decryption policy to “Immediately in Notification,” the decrypted message is displayed directly in the notification.

If users do not want the Passcode Identity message text to show in notifications that appear on the device Lock screen, they can configure their device’s notification settings to hide the text until they explicitly take

action to show it. The app online help provides information on how to configure device settings (see Passcodes > Hide sensitive information in notifications).

Changed

Identity as a Service account password reset allowed only if PIN Required policy is “true” (IDGM-10415)

Users are denied access to the Identity as a Service account password reset feature if the Identity Provider’s policy for Soft Tokens does not require tokens to be protected with a PIN. The FAQ in the app help provides details for users.

Length of token name increased (IDGM-10435)

The maximum length of a Token Identity name was increased from 20 to 50 characters.

Fixed

(IOS) PIN Reset Code overlaps Token Identity serial number on non-English screens (IDGM-10513)

This occurred if the text size was set to maximum. This issue has been resolved.

Telephone number truncated after 9 digits (IDGM-10458)

When entering a telephone number to register for a Passcode Identity, the app automatically dismissed the keyboard after the 9th digit for Italian phone numbers. This has been resolved so the keyboard is dismissed only after the 10th digit is entered for Italian phone numbers.

(iOS) End-user License Agreement (EULA) text was not displayed if font size set to large (IDGM-10478)

Users must agree to the EULA text to use the app. The font size for the app has been limited to ensure that the entire EULA text is displayed.

(iOS) Cancel button missing on screen for completing Passcode Identity activation (IDGM-10445)

This issue has been resolved.

System updates

Important information for organizations using Entrust Identity Enterprise

See System updates in Release 22.11.0

Release 22.3.1

Changed

End user license agreement added (IDGM-10186)

With Entrust Identity mobile app release 22.3.1 (and newer) users must agree to the terms of the End User License Agreement (EULA) to use the app. The EULA is displayed the when the app is first opened after initial installation or upgrade. If the terms of the EULA change in a future app release, users will be asked to accept the EULA again.

Fixed

First OTP is invalid (IDGM-10362)

A bug was resolved where an old token OTP was displayed when the app was opened from the background.

Incomplete transaction summary is displayed (IDGM-10398)

The pending transactions screen now displays more of the transaction summary. In previous versions the summary was being cut off.

Release 22.3.0

Changed

(iOS only) Limit on size of logs (IDGM-10073)

Previously there was no limit on the size of the log file in the iOS version of the app. The log file is now limited to 10 MB.

(Android only) Root detection updates (IDGM-10279)

The root detection capabilities have been updated.

Fixed

(iOS only) App closed unexpectedly after scanning QR code (IDGM-10375)

This behavior occurred if the QR code did not contain an Identity Provider URL. This issue has been resolved.

Drop-down notification was not cleared (IDGM-10382)

The drop-down notification was not cleared after a user opened the app manually and opened the notification from the **Actions** icon. This issue has been resolved.

Release 22.2.0

New features and enhancements

(Android) Log4j replaced with TinyLog (IDGM-9350)

TinyLog is now used for the app's message logging.

(iOS) Users can select the application to use to send log files (IDGM-6455)

Previously, the iOS mail application was the only one used to send log files. The app now offers a choice of apps to use when sending the log files.

App did not allow a retry if wrong OTP was entered to register Passcode Identity (IDGM-9977)

Previously, if a user entered the wrong OTP or if the OTP expired when creating a Passcode Identity, the user had to begin the process again. Now, if the OTP expires, the same OTP is sent again. If an incorrect OTP is entered, a new OTP is sent. The actions allow the user a chance to retry the registration.

Performance improvements (IDGM-9007)

The app's performance is improved with the following changes:

- Set the network request timeout for Android and iOS to 10 seconds

- Run Soft Token transaction polling in parallel

Token Identity login screen improvements (IDGM-9818)

Improvements to the way users are prompted to authenticate to unlock a Token Identity. These improvements make the user's required action clearer.

Improved message about how to grant camera permission for QR codes (IDGM-9870)

For users who did not grant the camera permission to capture QA codes when installing the app, a more informative message explains how to grant this permission when it is required to scan a QR code.

Changed

Authenticator deleted after entry of 10 incorrect unblock codes (IDGM-8554)

If a user attempts to unblock an Identity PIN and enters the Unblock Code incorrectly 10 times, the authenticator is deleted.

(iOS) App requests Bluetooth permission only if user has Smart Card Identities (IDGM-9849)

Previously, the app would ask for permission to use Bluetooth even when not required. It is required only to support Smart Card Identities.

Fixed

(iOS) Could not send logs from iPhone except from iOS mail app (IDGM-9953, IDGM-6455)

The iOS mail application was the only one that could be used to send log files.

Buttons not visible on some mobile device screens (IDGM-10146)

In some scenarios (for example, sign-in, manual token activation) users were unable to see the buttons they needed to select to proceed. The screen content is now scrollable when the font size or presence of the keyboard prevents all screen content from being visible initially.

System updates

The minimum supported iOS version was changed from 12 to 13.

Release 21.12.1

- **Push Notification without Confirm/Cancel Button (IDGM-10129)**

  After users get a transaction notification, they are unable to confirm it since the "Confirm" button is not present. This issue has been resolved.

- **Computer pairing with Android phone unsuccessful on some devices (IDGM-10058)**

  If a Smart Card Identity was deleted, the reference to it for the Auto-Connect Identity and the Passwordless logon was not cleared properly. This issue has been resolved.

- **Incorrect Danish translation on the Token Identity login screen (IDGM-10096)**

  The **Unlock** button on the Token login screen used the incorrect translation in Danish. It says "Lås" (Lock) instead of "Lås op" (Unlock). This issue is resolved in release 22.2.0.

Release 21.12.0

New features and enhancements

- **Integration of the SMS Passcode mobile app as Passcode Identities in the Entrust Identity mobile app**

  The Entrust Identity mobile app will immediately replace the legacy SMS Passcode app. Existing users will be able to continue using the old app to receive messages however they will no longer be able to use the old app to provision phone numbers. New Entrust Identity Essentials users must use the Entrust Identity mobile app to provision their phone numbers (activate their Passcode Identity).

  With the new Identity type in the app, Entrust Identity Essentials (formerly SMS Passcode) users will be able to use their Passcode Identity to do the following things:

  - Authenticate to websites, applications, or computers protected by their Identity Provider (user of Entrust Identity Essentials) with a one-time passcode sent to the app.
  - Receive other information from their Identity Provider, such as a lockout notification or reminder to change an account password.

- **Support for Danish, Norwegian, and Swedish (IDGM-6193)**

  This release adds support for these three languages.

Changed

- **PIN or biometric authentication required before viewing Smart Card Identity action history (IDGM-9932)**

  When accessing a Smart Card Identity's details, users are prompted to unlock the Smart Card Identity. If the Entrust Identity policy is set to **Session**, users are not required to unlock the Smart Card Identity again until the session has expired. If the policy is set to **Transaction**, users must unlock the Smart Card Identity every time they want to see a Smart Card Identity's details.

  Relevant policies in each product:

  - Entrust Identity as a Service policy: **Smart Credentials > PIN Prompt**
  - Entrust Identity Enterprise policy: **Smart Credentials > Mobile Smart Credential PIN**

Fixed

- **Notifications not visible when some app screens were in focus (IDGM-9376)**

  Notifications received while the user was viewing some app screens (such as the Action History screen) were not displayed. This issue has been resolved.

Release 21.10.0

Features and enhancements

- **Entrust Identity mobile app supports Smart Card Identities**

  With this release, the Entrust Identity mobile app adds smart credentials as an authenticator type managed by the app. With this capability, the Entrust Identity mobile app fulfills most of the functions supported with the legacy Entrust IdentityGuard Smart Credentials app.

Smart credentials, or Smart Card Identities as they are called in the app, can be used to perform the following actions (see **Error! Reference source not found.** for details):

- Passwordless login to Windows and Mac computers
- Smart Login to resources protected by Entrust Identity as a Service
- Smart Card Identities also support many of the features described in **Error! Reference source not found.**, including protection with PIN and biometrics, transaction notifications, action history, and support for multiple Smart Card Identities.

For information about how to configure these capabilities, see the documentation for the Entrust product you are using. (In these documents, this kind of authenticator is called a smart credential.):

- Entrust Identity as a Service: *Entrust Identity as a Service Administrator Help*
- Entrust Identity Enterprise:
  - *Entrust Identity Enterprise 13.0 Server Administration Guide*
  - *Entrust Identity Enterprise 13.0 Smart Credentials Guide*

Fixed

- IDGM-9736 - One Time Password (OTP) was not displayed correctly in Arabic.
- IDGM-9653 - Tapping “Forgot your PIN?” did not do anything.
- IDGM-9352 - User could tap the Activate button multiple times when activating a Soft Token.
- IDGM-8831 - (iOS only) App became unresponsive at startup.
- IDGM-949 – (iOS only) Data in the KeyChain was corrupted resulting in the loss of Token Identities.

Release 21.5.0

Features and enhancements

- Transaction screen layout improved so action buttons could be viewed more easily.

Fixed

- Transaction details were cut off.
- Error message was displayed if the Identity Provider configuration did not have a logo URL.
- Soft token Identities were lost if the app was terminated while saving data.
- An ACTIVATEONLINECOMPLETE audit was generated in Identity as a Service every time a user opens the app.
- The app became unresponsive when launched from a notification.

Release 21.4.1

Fixed

- App stability fixes
- On Activation details screen, buttons not visible on phone with large font size or small screen.

Release 21.4.0

Fixed

- Device Tokens were not updated in the Identity Provider, which caused push notifications to stop working.

Release 21.3.2

Features and enhancements

- Added support for the Show OTP Deep Link action.
- Added support for Soft Token activation using encrypted activation parameters.

Fixed

- Soft Token Identity activation failed if there was no Transaction URL

Release 21.3.1

Features and enhancements

- Added support for manual Soft Token activation.

Fixed

- Soft Token activation failed if there was no Identity Provider URL.
- App closed unexpectedly when scanning a QR code for offline activation.
- (iOS only) App closed unexpectedly when migrating data from the legacy app.

Release 21.3.0

First release of this app.

Known issues and limitations

This section describes the known issues and limitations in this version of the Entrust Identity mobile app. Affected device types are shown in brackets where an item does not apply to all device types, Numbers in parentheses are for internal tracking purposes.

DNS Resolution Timeout (IDGM-14082)

When the DNS server is unresponsive, the (Android) application loading time may exceed one minute as it attempts to connect to the identity-associated backend. Initially, the application tries to connect to the identity backend to retrieve information. If a DNS resolution timeout occurs during this process, the application will wait until the timeout is triggered. This timeout, managed by Android Java, may last more than one minute.

Once the timeout is triggered, the application will proceed with the startup as usual. However, this behavior should not occur because the application requires a server connection to function correctly. If this issue arises, contact your provider to check for any performance degradation in their DNS servers.

Enable airplane mode to access the application quickly if an outdated identity points to a problematic domain that needs removal.

IMPORTANT: This known issue is related to a DNS resolution timeout, which is different from a server connection timeout, that is managed by the app.

(Android) App is closed and the Bluetooth connection is dropped when the app is in background (IDGM-12295)

Users must configure the setting described here to configure the phone properly and reduce the number of times the OS closes the app when it is in background.

1. Go to OS settings and click on “Apps”.
2. Search for the Entrust Identity App and click on it.
3. Search an option related to the “App battery” (it may differ between different phone brands) and select the “unrestricted” setting and restart the Entrust Identity app. By default, it is set to “optimized”.

The user needs to disable "Adaptive Battery" on Android settings

1. Open your Android device's settings.
2. Scroll down and tap on "Battery" or "Battery & device care," depending on your device.
3. Look for "Adaptive preferences" or "Battery optimization," and tap on it.
4. If you see "Adaptive Battery," tap on it.
5. Toggle off the switch to disable Adaptive Battery.

Note: The exact names of menus and options may vary slightly depending on your Android device's version and manufacturer.

(Android) Repeatedly receiving login notifications on mobile when both computer and mobile are left idle and CTRL+ALT+DEL usage is disabled on Windows to start the login process. (IDGM-12253)

During Smart Identity login process, if you do not have a user action as CTRL+ALT+DEL to start a login process, Windows automatically starts a new login process when previous one is cancelled due some timeout. If the user has the Smart Identity connected could start receiving login notifications while Windows is retrying the login process if the process is not completed by the user.

(iOS) Message decryption policy on Essentials notifications is not working on iOS 17 (IDGM-11909)

If you receive an Essentials notification on iOS 17 with decryption policy enabled, it will not be shown as expected. The user will need to access to the app to read the message. Other iOS versions prior to 17 are working as expected.

(iOS) Email subject not automatically entered if logs sent in email other than iOS mail client (IDGM-9953)

If you have not configured the iOS native mail application on your mobile device, you can choose another mail client to use to send log files, however, the subject line of the email is pre-filled only if using the iOS mail application.

(Android) Activating Smart Identity from QR code in email fails (IDGM-8879)

If an Identity Provider sends a Smart Identity activation link by email in the form of a QR code, the user should be able to tap the QR code in an email displayed on the mobile device where the Entrust Identity mobile app is installed to open the app and complete the activation. On some Android devices, tapping the QR code does not open the app.

Workaround: Users can open the email on a different device (for example, a computer), and scan the QR code using the app.

Update feature does not update a Smart Identity with certificates that have expired or been revoked (IDGM-9198)

If a certificate in a user's Smart Identity has expired or been revoked, the user cannot use the **Update** button in the Entrust Identity mobile app to update it. The user must use the smart credential update option on the Identity Provider's self-service website to do the update. If the user has a derived Smart Identity with certificates that have expired or have been revoked, the user should delete the derived Smart Identity and create a new one. This is described in the "Update a Smart Identity" topic in the app help.

(Oppo phones with ColorOS) Push notifications are not received when the app is closed (IDGM-7164)

Users must configure the settings described here to be able to receive push notifications when the Entrust Identity mobile app is not running on their Oppo phone.

1. Open the device settings and select **Battery > Energy Saver**. Select the Entrust Identity mobile app, then enable the **Do not optimize** option.
2. Still in the settings, select **Battery > Battery optimization**. Select the Entrust Identity mobile app, then disable the following options: **Freeze when in Background** and **Automatically Optimized when abnormality is Detected**.
3. Still in settings, navigate to **Notification & Status Bar > Notification Manager**. Select the Entrust Identity mobile app, then enable all the options *except* **Hide content of notification on the lock screen**.
4. Open the **Security** app and navigate to **Privacy permissions > Startup Manager**. Enable the Startup Manager for the Entrust Identity mobile app.

(iOS) Apple end of support for SHA-1 can result in error message in app (IDGM-2636)

Apple platforms have deprecated aging hashing algorithms and cryptography standards. Certificates signed with SHA-1 and/or using private keys under 2048-bits are no longer trusted on High Sierra, iOS 11, watchOS 4, or tvOS 11. For users of the Entrust Identity mobile app on devices with iOS11 (or later) installed, this means that the app cannot communicate with domains that have a certificate signed with SHA-1 or that use private/public keys of less than 2048 bits. In this case, the app displays the following error message: "Certificate validation error communicating to <identity provider domain>. Contact your identity provider."

Resolution: Replace the certificate on your website with one that supports newer hashing algorithms and cryptography standards.

Installation notes

Installation of the app on user devices

Users of iOS devices must obtain the Entrust Identity mobile app directly from the Apple App Store.

Users of Android devices can obtain the Entrust Identity mobile app directly from Google Play.

When the Entrust Identity mobile app is installed, it requests the following permissions:

- Take pictures and videos - to scan QR codes for activation or transaction verification, and to use facial recognition features.
- Bluetooth – to connect to a computer for Smart Identity login.

Customer support

Entrust recognizes the importance of providing quick and easy access to our support resources. The following subsections provide details about the technical support and professional services available to you.

Technical support

Entrust offers a variety of technical support programs to help you keep Entrust products up and running. To learn more about the full range of Entrust technical support services, visit our Web site at: http://www.entrust.com/

If you are registered for our support programs, you can use our Web-based support services.

Entrust TrustedCare Online offers technical resources including online versions of Entrust product documentation, white papers and technical notes, and a comprehensive Knowledge Base at: https://trustedcare.entrust.com

If you contact Entrust Customer Support, please provide as much of the following information as possible:

- Your contact information
- Product name, version, and operating system information
- Your deployment scenario
- Description of the problem
- Copy of log files containing error messages
- Description of conditions under which the error occurred
- Description of troubleshooting activities you have already performed

Telephone numbers

For support assistance by telephone call one of the numbers below:

- 1-877-754-7878 in North America
- 1-613-270-3700 outside North America

For telephone assistance in obtaining Web server certificates call one of the numbers below:

- 1-866-267-9297 in North America
- 1-613-270-2680 outside North America

Email address

The email address for Customer Support is: support@entrust.com. Product installation or support issues must be opened with Customer Support.

Feedback concerning documentation can be directed to http://go.entrust.com/documentation-feedback.

Online support

To submit a question online, go to http://www.entrust.com

Professional Services

The Entrust team assists e-businesses around the world to deploy and maintain secure transactions and communications with their partners, customers, suppliers, and employees. We offer a full range of professional services to deploy our e-business solutions successfully for wired and wireless networks, including planning and design, installation, system integration, deployment support, and custom software development.

Whether you choose to operate your Entrust solution in-house or subscribe to hosted services, Entrust Professional Services will design and implement the right solution for your e-business needs. For more information about Entrust Professional Services please visit our Web site at: https://www.entrust.com/services/.