Quick Heal Version 1.3

Revision 1.5 | Dec 4, 2024

Quick Heal AntiFraud.AI

Version 1.3

Release Notes| Dec 4, 2024

Contents

Revision History

Doc Version	Date	Comment	Platform (Mobile/ Desktop)	Features Section Link	Build Info Section Link
1.5	4th Dec, 2024	Quick Heal Desktop AntiFraud released with multi-device package	Desktop v1.2	New Features and Enhancements	Build Information DAF v1.2
1.4	26th Nov, 2024	Quick Heal Mobile AntiFraud released with multi-device package	Mobile v1.3	New Features and Enhancements	Build Information MAF v1.3
1.3	13th Nov, 2024	Quick Heal Desktop AntiFraud released with Free Trial package	Desktop v1.1	New Features and Enhancements– DAF v1.1	Build Information AF v1.1
1.2	9th Nov, 2024	Quick Heal Mobile AntiFraud released with Free Trial package	Mobile v1.2	New Features and Enhancements– MAF v1.2	-
1.1	25th Oct, 2024	Quick Heal Mobile AntiFraud released	Mobile v1.1	New Features and Enhancements– MAF v1.1	-

1.0	4th Oct, 2024	Quick Heal AntiFraud for mobile and desktop launched	Mobile v1.0 + Desktop v1.0	Features – MAF v1.0 Features – DAF v1.0	Build Information AF v1.0

Abstract

The Quick Heal Build Release Notes includes the following information of the released builds:

- Build Information
- New Features and Enhancements
- Known Issues
- Bug Fixes
- Deferred List
- System Requirements

Build Information DAF v1.2

Refer to the following build information for the desktop AntiFraud release **1.2.**

Product Name	Build VDB	Build Version	MD5 Checksum	
			32-bit build	64-bit build
Quick Heal AntiFraud - Desktop	27-November-2024	25.0.0.2	cc794896617dceb8f6fa42748079cc63	16112f3b506e44561436fbf9ac9970d1

Build Information MAF v1.3

Refer to the following build information for the mobile AntiFraud release **1.3.**

Product Name	Build VDB	Build Version	MD5 Checksum	
Quick Heal AntiFraud - Mobile	13-November-2024	1.3	NA	NA

Build Information DAF v1.1

Refer to the following build information for the desktop AntiFraud release 1.1.

Product Name	Build VDB	Build Version	MD5 Checksum	
			32-bit build	64-bit build
Quick Heal AntiFraud - Desktop	20-September-2024	25.0.0.1	21f9345bcb6e4a65fa206e9a77a88900	4009afb7bfcd78b6f789f3fe81ada2a3

Build Information DAF v1.0

Refer to the following build information for the desktop AntiFraud release 1.0.

Product Name	Build VDB	Build Version	MD5 Checksum	
			32-bit build	64-bit build

Quick Heal AntiFraud - Desktop	20-September-2024	25.0.0.1	270c278b8e91128e03c5aa8b2bdd11d7	4eed2eb5b2bbad91d39a78b46b9a7129

New Features and Enhancements

1. **Multi-device Subscription**
    - The multi-device subscription allows families or small groups to share a single product key across multiple devices, offering a cost-effective and streamlined solution. Rather than purchasing individual licenses for each device, users can manage access under one product key, simplifying setup and reducing overall costs.
    - This feature designates the first user as the Primary User, who oversees the group's access to the subscription. The Primary User can easily transfer licenses between devices without the need to purchase additional ones. This centralized control enables secure and flexible sharing, making it an ideal solution for households or small teams.
    - Building on the single-user sign-up process, the multi-device subscription allows users to purchase a license for either 3 or 5 devices. Additional users require the Primary User's consent for access. Once the maximum number of licenses is reached, the Primary User must verify new users via a code and has the option to transfer an existing license to another device.
    - You can use the same primary email to activate all devices slots within a multi-device key. There is no requirement for multiple emails.

Feature in Detail

Click here to view the feature demo, where its functionality is explained and instructions on how to use it are provided.

New Features and Enhancements – MAF v1.2

With this release, a Free Trial package is made available for the users.

- The first three months of the subscription are provided free of charge.
- The Annual subscription fee of ₹700 will be charged at the end of free trial period.
- The free trial package is not offered to users subscribing to the half-yearly, quarterly, or one-time, one-year plans.
- The 3-month free trial is available only to subscribers who purchase their subscriptions through the App Store or Play Store.
- Cancellation can be done at any time, and the user will not be charged the annual fee at the end of the subscription period. However, even after cancellation, the user will retain access to the product for the remaining duration of the subscription period.
- The subscription can be transferred to a new device. Once the transfer is complete, it will be deactivated on the previous device. Authentication will be sent to the primary email address, which is required to complete the transfer.

Feature in Detail

Click here to view the feature demo, where its functionality is explained and instructions on how to use it are provided.

New Features and Enhancements – MAF v1.1

Following is a list of Mobile AntiFraud enhancement introduced in MAF release v1.1:

1. Battery Optimization Whitelisting
    - A prompt will appear when battery optimization revokes accessibility permissions.
    - Upon the second app launch, the user will be prompted again if the permission remains revoked.
2. Force Upgrade Mechanism
    - Users are restricted from accessing the app if they are using an outdated version.
    - The app redirects users to the app store for an update.
3. Accessing Location in Background
    - The app verifies background location permission.
4. After making an in-app purchase, payment acknowledgment is received at the app's launch.
5. Cloud Interface for reporting fraudulent numbers.
    - Users have the ability to flag numbers as fraudulent.
    - The report is submitted to the cloud database for processing.
    - Users receive confirmation upon submission, and additional validation is conducted by the fraud team.
6. Fraud App Detector
    - Hidden apps must be excluded from the pre-burn app, ensuring that no system or pre-burn hidden apps are displayed.
7. Banking Fraud Alert
    - Scans for and alerts users about fraudulent SMS messages.
    - Identifies messages that appear to be from a bank regarding amounts credited to the account but are actually sent from a private mobile number rather than an official SMS service and notifies users of the potential fraud.
8. Secure Payment > Scanning Environment During Payment App Launch
9. The environment is scanned upon launching the payment app.
    - If secure, a "Scan Success" prompt will be displayed once per day for each application.
    - For subsequent attempts, scans will occur in the background without prompting the user for the remainder of the day.
    - If the environment is deemed insecure, a prompt will be shown each time.
    - The "Select All Apps" option will be removed from the "Add Apps" feature.
    - For customers in India, only a predefined selection of apps will be added.
10. Dashboard > Color changes based on Risk Score

11. Whitelist Number from Spam List in AntiFraud Application

    - Once a number is whitelisted, the user will no longer receive AntiFraud prompts for that number and will be unable to report it again.

Features – MAF v1.0

Following is a list of Mobile AntiFraud features introduced in this release:

1. **Fraud Protect Buddy**

   Helps users in adding a loved one as a dependant and protecting them from banking frauds.

2. **Fraud Call Alert**

   Helps users by providing alert notifications on receiving a potentially fraudulent call.

3. **Secure Payments**

   Helps in checking the payment environment and securing all online transactions from frauds.

4. **Call Forwarding Alert**

   Helps in providing alerts when the calls are being redirected to another number.

5. **Unauthorised Access Alert**

   Helps in providing alerts when Mic/Cam is being accessed while the device is not in use.

6. **Banking Fraud Alert**

   Helps in providing alerts when a call may potentially lead to fraud.

7. **Payee Name Announcer**

   Helps the user avoid QR code scams.

8. **Scam Protection**

   Protects users from phishing link scams.

9. **Fraud App Detector**

   Helps in providing alerts on detecting a fraud app.

10. **Dark Web Monitoring**

    Helps in providing alerts if your sensitive data is leaked on the dark web.

11. **Screen Share Alert**

    Helps in providing alerts if your screen is being shared, while on a call.

12. **Info Hub**

    Provides additional information on the latest market trends in cybersecurity through videos and articles, increasing awareness and helping users protect themselves from fraud.

13. **Victim of a Fraud?**

    Provides a step-by-step guide to assist users in reporting fraud.

Features – DAF v1.0

Following is a list of Desktop AntiFraud features introduced in this release:

1. **Scam Protection**

   Keeps you safe by blocking access to malicious and fraudulent websites.

2. **Dark Web Monitoring**

   Keeps an eye on your data to catch any potential leaks before they become a problem.

3. **Safe Banking**

   Launches your entire banking session in a secure environment, safeguarding all your vital data.

4. **Spy Alert**

   Keeps your privacy intact by blocking websites from tracking your online activities and using your preferences to influence your decisions.

5. **Webcam Protection**

   Scans for malicious apps and software trying to access your device's webcam, keeping your privacy secure.

6. **Backup & Restore**

   Offers secure data backups, efficient backup management, and seamless data restoration.

7. **Browsing Protection**

   Blocks access to infected websites from your browser.

8. **File Vault**

   Saves confidential and important data such as documents, files, photos, videos, and any other data in an encrypted format to prevent unauthorized access.

9. **Email Protection**

   Configures the protection rules for all incoming emails. These rules include blocking infected attachments (malware, spam and viruses) in emails.

Known Issues

Following is a list of known issues identified in Desktop AntiFraud:

1. To ensure the proper coexistence of Quick Heal AntiFraud with Quick Heal Antivirus, it is essential that the antivirus is updated to version 25. If the antivirus is not at this version, functionality may be compromised.
2. **Spy Alert:** Is supported only for Microsoft Edge Chromium, Mozilla Firefox version 52.9.0 and above, and Google Chrome version 63 and above.
3. **Browser Sandbox:** This feature does not support older versions of Microsoft Edge browser of Windows 10 and Windows 11 operating systems and Mozilla Firefox 64-bit.
4. **Self-Protection:** Microsoft System Restore will not work if Quick Heal Self Protection is enabled. Before performing System Restore, it is recommended to turn Quick Heal Self Protection off. To turn Quick Heal Self Protection off, follow these steps:
    a. Open Quick Heal AntiFraud.
    b. Go to More > Settings. Set Self Protection off.
5. Password Protection settings will not be exported when you export it to a file. These settings have to be configured manually after re-installation.
6. Installation of WinPKFilter (Windows Packet Filter) is not recommended if Quick Heal AntiFraud is already installed on your computer. Installing WinPKFilter on the same machine may result in improper functioning of Quick Heal AntiFraud.
7. An interoperability issue with WinGate Proxy Server may cause a system to crash with Blue Screen Error or BSOD if WinGate Proxy Server is installed after Quick Heal AntiFraud installation. It is recommended to install WinGate Proxy Server before Quick Heal AntiFraud installation to avoid the interoperability issue.
8. In-App purchase flow for Buy Now requires Microsoft Edge on Win 8 and Win 8.1 operating systems.

Following is a list of known issues identified in Mobile AntiFraud:

- The **SMS and WhatsApp Scam Protection** feature in the AntiFraud App may not work if notifications for these apps are disabled or not visible on the device.
- Certain features of the AntiFraud App may be limited on **Android Go Edition** devices due to hardware or OS constraints.
- The **Accessibility**, **Draw Over Other Apps**, and **Read Call Logs** permissions are mandatory for the AntiFraud app. If these permissions are not granted or not available on any Android device, the associated features will not function as expected.
- On **iOS**, if the app is in a **closed state** or running in the **background**, users may not receive real-time notifications or alerts.

- In the **Fraud Protect Buddy** feature, an **Apple user** can only act as a **Buddy** and cannot be added as a **Dependant**.

Bug Fixes

These are the issues that were fixed in this release.

Sr. No.	ID	Description
1	MAF-3811	Android | Some of authentic apps detected under Fraud App Detector
2	MAF-3806	Android | Email app not visible when sharing logs
3	MAF-3804	Android | Getting "UK" as profile where user has no UK in their name or email while activating product
4	MAF-3803	Android | High risk pill seen as amber instead of red when scroll under dark web monitoring
5	MAF-3756	Payee Name is not working
6	MAF-3730	Android | 'AntiFraud' Failed to start several times.
7	MAF-3801	Android | Fraud call alerts | Sentence correction when reporting a number as fraud

Deferred List

The following is a list of items that have been deferred and would be included in future releases.

Sr. No.	ID	Description
iOS Limitations		
1	MAF-3039	Installed OS Update (Risk Level) – There is no public API provided by Apple for updating the operating system. Operating system updates are restricted on older devices, and there is no straightforward method to verify if a device is running the latest OS version. A private repository exists detailing the maximum supported OS version for each device model. Consequently, this limitation imposed by Apple will be handled in the subsequent release.
2		Fraud Call Alert – Once the repository is created on Android/third party platform, the functionality should work as expected. Expect a delay of up to 24 hours due to absence of an event of a call.
3		
4		

System Requirements

To use Quick Heal AntiFraud, you must ensure the following requirements are met.

Device Requirements for installing AntiFraud on Mobile

- Android OS 10 or above;
- iOS version 14 or above.

General Requirements for installing AntiFraud on Desktop

- 2.9 GB disk space for Quick Heal AntiFraud
- 4 GB and above RAM
- Internet Explorer 6 or later
- Internet connection to receive updates
- Minimum screen resolution 1024 * 768

System Requirements

Desktop operating system: Microsoft Windows 11, 10, 8.1, 8 fully patched (32- and 64-bit)

Note:

- The requirements are applicable to all flavors of the operating systems.
- The requirements are applicable to the 32-bit and 64-bit operating systems unless specifically mentioned.
- System requirements may change from time to time. It is advisable to check the latest system requirements at www.quickheal.com.

Supported POP3 Email Clients

Quick Heal AntiFraud supports the following email clients.

- Microsoft Outlook Express 5.5 and later
- Microsoft Outlook 2000 and later
- Netscape Messenger 4 and later
- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail

Note:

- The Email Protection feature does not support encrypted email connections that use Secure Sockets Layer (SSL).
- IPV6 protocol is not supported by Quick Heal AntiFraud.

Technical Support

Quick Heal provides extensive technical support for the registered users. To see the support options, follow these steps:

1. Open Quick Heal AntiFraud.
2. On the left pane, click the **More** option and then select the **Support** option.

Support by Phone

Customers based in India can dial Toll Free number: 1800-121-7377.

To know a relevant contact number, customers from outside India should visit:

www.quickheal.com/contact_support.

Other Sources of Support

To get other sources of support, please visit www.quickheal.com/support-center-faqs.