Wickr Enterprise Client
Common Criteria Evaluated Configuration Guide (CCECG)

Version 1.0
Revision Date: March 6, 2023

Table of Contents

Introduction

The Wickr Enterprise Client 6.10 includes stand-alone executable clients for Windows, Linux, Mac OS, iOS, and Android systems. These clients are installed on endpoint systems in an organization to facilitate peer communications. The Wickr Enterprise Client interacts with an environmental Wickr Enterprise Server that is used for administration of the Wickr Enterprise Client and communication control. The platform-specific versions of the TOE include:

1. Wickr Enterprise Client for Windows 6.10.0

   Evaluated on Microsoft Windows 11.

2. Wickr Enterprise Client for Linux 6.10.1

   Evaluated on Ubuntu 18.04.

3. Wickr Enterprise Client for macOS 6.10.2

   Evaluated on macOS 11.

4. Wickr Enterprise Client for iOS 6.10.0

   Evaluated on iOS 15.5.

5. Wickr Enterprise Client for Android 6.10.0

   Evaluated on Android 12.

This document provides supplementary details on how to configure and manage the Wickr Enterprise Client 6.10 so that mandatory functionality prescribed by the App PP are provided. These details supplement those provided in the following product documentation:

- Wickr Enterprise: Installation and Maintenance v6.10
- Wickr Enterprise Administrator Guide v6.10
- Wickr Enterprise Desktop User Guide v6.10

Document Purpose and Scope

This document provides supplementary administrative guidance for the Wickr Enterprise Client 6.10.

This document describes procedures on how to operate and prepare the Wickr Enterprise Client 6.10 to meet its Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Application Software Protection Profile v1.4 [SWAPP], and supplements the other product documentation listed above to meet the required guidance assurance activities.

TOE Description

Evaluated Configuration

The Wickr Enterprise Client TOE is an on-premise software application providing communication with remote peers and runs on the following platforms:

- Windows
- Linux
- macOS
- iOS
- Android

The Wickr Enterprise Client is part of a client-server distribution that interacts with the Wickr Enterprise Server application in its operational environment. Collectively, they make up the Wickr Enterprise solution. The Wickr Enterprise Server application is not included in the TOE.

Users join the Wickr Enterprise Network by downloading a free copy of their platform's Wickr Client application and subscribing to the Enterprise Network by paying a monthly subscription fee. Upon establishing a subscription, the User's Wickr Client receives configuration information from a Wickr Server, enabling connection to the Wickr Enterprise Network. Wickr Servers are part of the infrastructure supporting the Wickr Enterprise Network. They exchange user information and routing information to enable messages to traverse the network from Server to Server until the final Client is reached.

All Wickr Clients communicate through Wickr Servers for client-to-client communication. The 'base' configuration of the Wickr Server runs as a Messaging Server. Wickr Client to Client communication is actually Wickr User/Wickr Client to Wickr User/Wickr Client communication. A registered Wickr User may be registered on multiple platforms (Client instances) and a Wickr Server may have multiple Wickr Users registered on its system. The Wickr Messaging Server is responsible for authenticating Wickr Users and discovering routing information. On receipt of a connection request, once authenticated, the Messaging Server discovers information about the recipient(s) by configuration information.

Administration of the Wickr Enterprise Network is by Web access to the Messaging Server. The Messaging Server sends configuration information to Wickr Enterprise Clients in the form of configuration files. Additionally, Wickr Users may manage a limited set of parameters about their Wickr Client accounts.

The Wickr Enterprise Client interacts with the underlying platform when using its network connectivity. Network usage of the TOE is authorized implicitly through user guidance; it does not make any specific requests on its own to use network services once installed. The TOE uses network connectivity to interact with a Wickr Server to establish connections with other Wickr Clients (via Wickr Server); inbound message/call; for remotely-initiated push notifications for incoming connections (iOS and Android); and to check for application updates (Android, iOS, macOS, and Windows).

In support of peer connections, the TOE may access the following platform resources: location services, photos, and address book.

The Wickr Client uses platform-provided cryptographic services for protection of locally-stored credential data. No configuration is required to activate these services.

Note: The TOE is the Wickr Enterprise Client software only. The host platforms and the Wickr Enterprise Server are not included in the TOE.

Physical Boundaries

The TOE consists of the Wickr Enterprise Client 6.10 application. The platform-specific versions of the TOE include:

1. Wickr Enterprise Client for Windows 6.10.0

   Evaluated on Microsoft Windows 11.

2. Wickr Enterprise Client for Linux 6.10.1

   Evaluated on Ubuntu 18.04.

3. Wickr Enterprise Client for macOS 6.10.2

   Evaluated on macOS 11.

4. Wickr Enterprise Client for iOS 6.10.0

   Evaluated on iOS 15.5.

5. Wickr Enterprise Client for Android 6.10.0

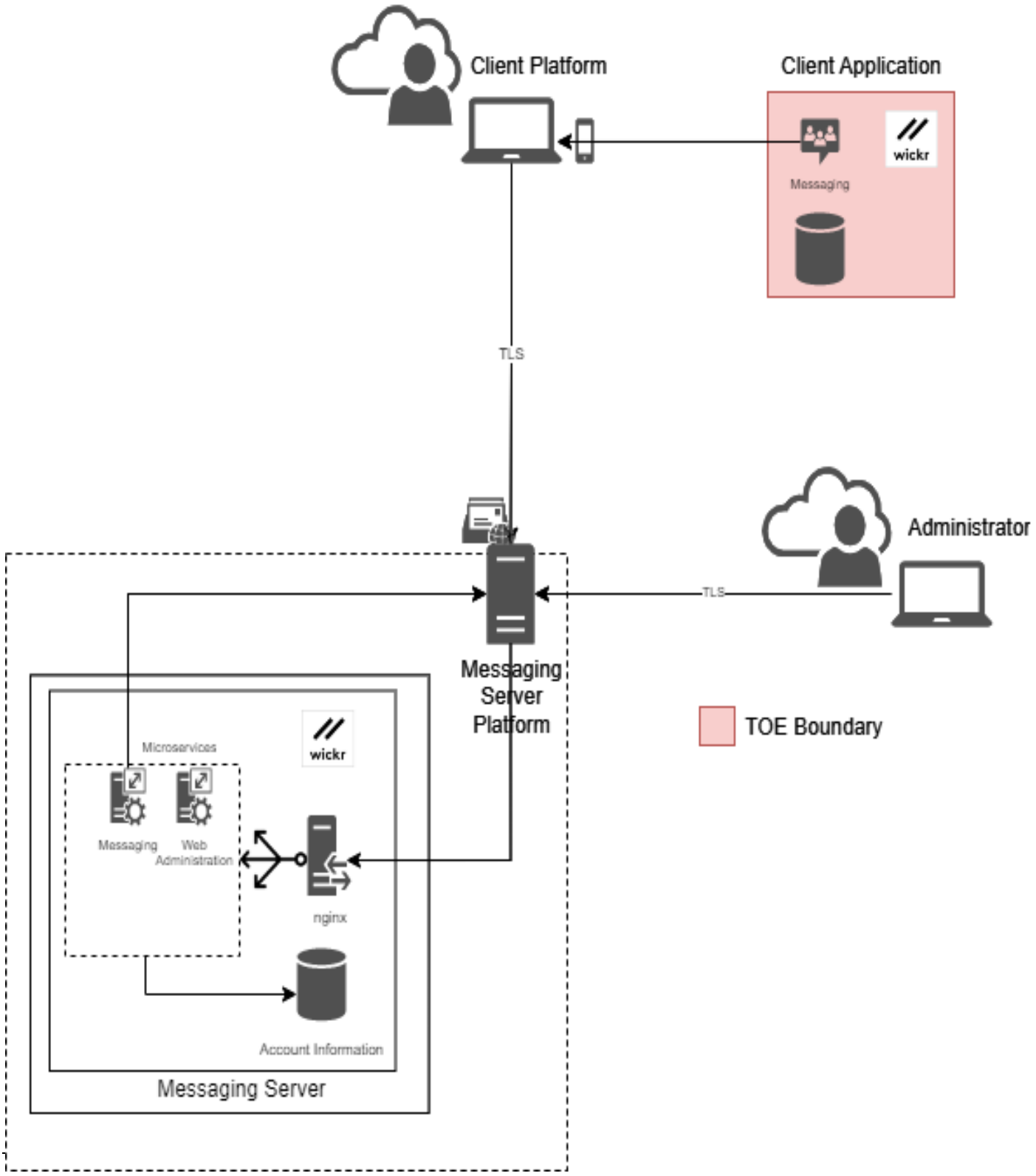
   Evaluated on Android 12.

In addition to the platforms identified above, the TOE's operational environment includes the following:

- A Wickr Server installed for messaging
- One or more remote Wickr Client instances to establish connections with
- A Workstation with a browser to access the Wickr Server's Admin Console. (Wickr Clients receive configuration information from a Wickr Server)
- An Update server (public download site).

The product architecture is shown in the following figure. The Wickr Client application (the TOE) is indicated by the red box. The other items are implemented on the Wickr Servers and other systems that are part of the TOE's Operational Environment.

The figure depicts initial communication setup for a call. The direction of the arrows indicates which system initiates communication. Communication is bidirectional once a connection is established. The Wickr Client relies on the cryptographic functions of its host platform for data in transit.



Logical Boundaries

The TOE provides the security functionality required by [SWAPP].

The Target of Evaluation (TOE) for the Wickr Enterprise Client 6.10 consists of the mandatory functionality prescribed by the App PP, as well as some selection-based functionality where needed.

The logical boundary is summarized below. In general, the following Wickr capabilities are considered to be within the scope of the TOE:

- Trusted communications between Wickr Client and Wickr Server.
- The extent to which the TSF relies on platform-provided and third-party capabilities to perform its functionality.
- The extent to which data used to determine the behavior of the TSF is secured while at rest and in transit.
- The ability for the TOE to function on a host platform that is configured for secure operation.
- The ability of the TOE to interface with the low-level components of its host platform in such a manner that the TOE cannot be used as an attack vector to exploit the host platform.
- The ability of the organization deploying the TOE to perform timely and trusted security updates to it.

Assumptions

The following assumptions were drawn from the [SWAPP].

Assumption	Description
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

Excluded From the Evaluation

The following functionality is excluded from the Common Criteria evaluation.

Excluded Functionality	Description

Excluded Functionality	Description
Voice and Video Services (Conferencing Server)	The TOE includes the base text messaging services only.

Software Download, Installation and Configuration

Download and Installation

Users join the Wickr Enterprise Network by downloading a free copy of their platform's Wickr Client application and subscribing to the Enterprise Network by paying a monthly subscription fee. Upon establishing a subscription, the User's Wickr Client receives configuration information from a Wickr Server, enabling connection to the Wickr Enterprise Network.

For macOS and Windows platform versions of the TOE, the user obtains the application software through the vendor's support site as identified in the Wickr Enterprise Desktop User Guide Section "*Download Wickr Enterprise*". The Android and iOS platform versions of the TOE are obtained from their respective app stores; while the Linux version of the TOE is obtained from the Ubuntu Software Centre. Once the Wickr Server administrator has created a Client Config File as described in the Wickr Enterprise Administrator Guide, Section "*Client Configuration*", the client can register and establish a connection to the Enterprise service. Users must have a valid username and password to complete the Registration and Sign In process. The user's administrator provides the login URL as well as a temporary username and password. The user registration process and screenshots are shown in the Wickr Enterprise Desktop User Guide "Desktop Registration" section.

Once the TOE is in an operational state and connected to the Wickr Server, the server can interface with the client to communicate configuration changes through a JSON API on the client. Specifically, the server can be used to configure the number of authentication failures that are allowed for a user to access the client. This is performed from the Security tab as described in the Wickr Enterprise Administrator Guide.

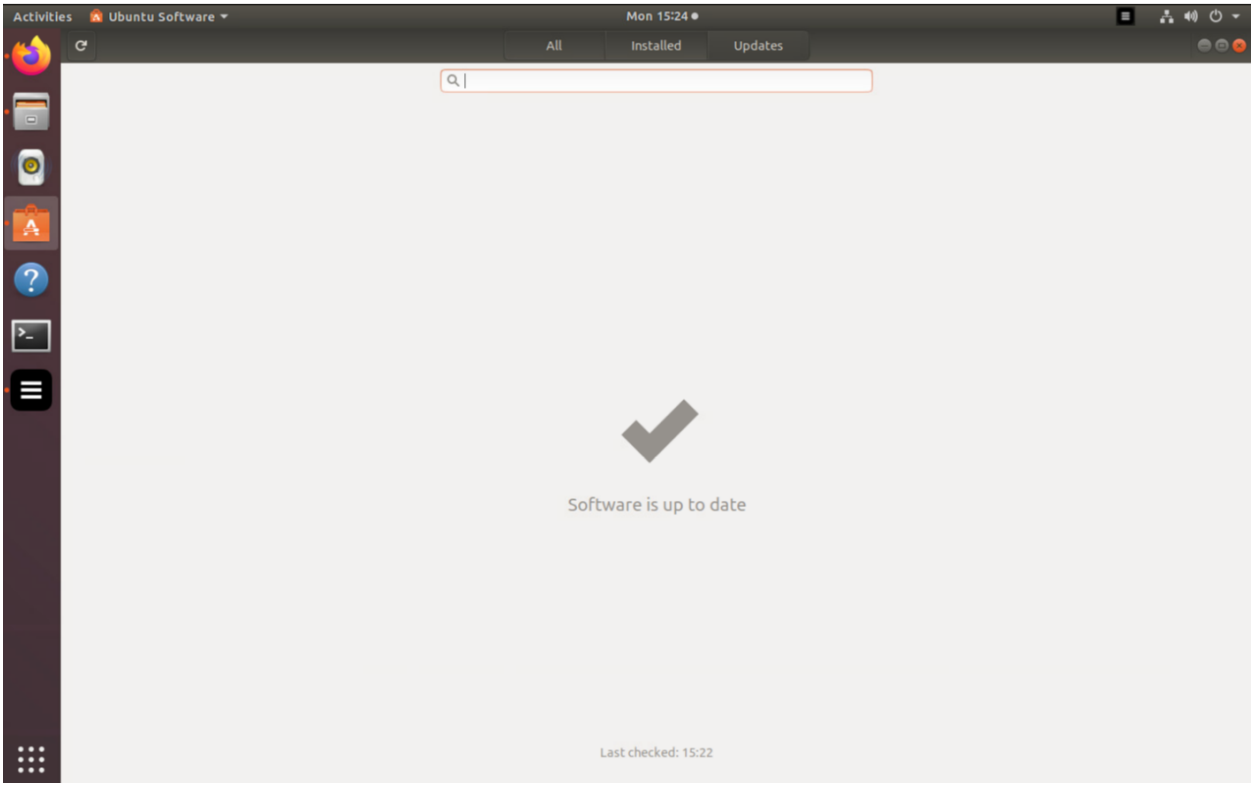
Wickr regularly releases new versions of its software which are deployed according to the customer's requirements.

The macOS and Windows platform versions of the TOE periodically check for updates on the vendor's support site. The Android and iOS platform versions of the TOE periodically check for updates through a check by the TOE to their respective app stores. For these platforms, updates are checked hourly. For the Linux platform version of the TOE, the update check is handled entirely by the platform through the

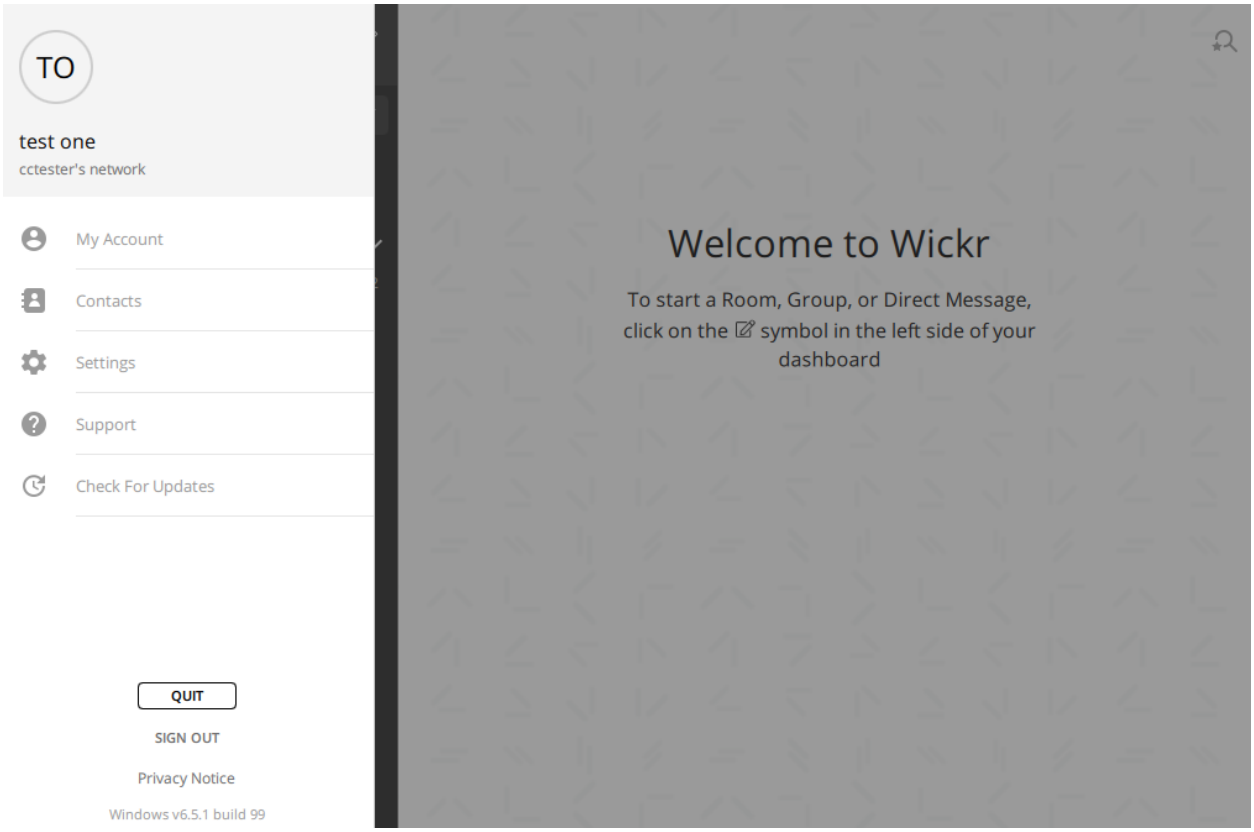
Ubuntu Software Centre. Regardless of the platform version, the TOE never downloads, modifies, replaces, or updates its own binary code. Updates to the TOE are always performed by the platform.

The user can check for an update on the Ubuntu platform by performing the following steps:

1. Open the Ubuntu Software app (placed in the dock on a default Ubuntu install, or can be found in the app list – the "waffle" in the bottom-left corner).
2. Tab over to Updates along the top bar, and check the list. Refresh using the button on the top-left if necessary.

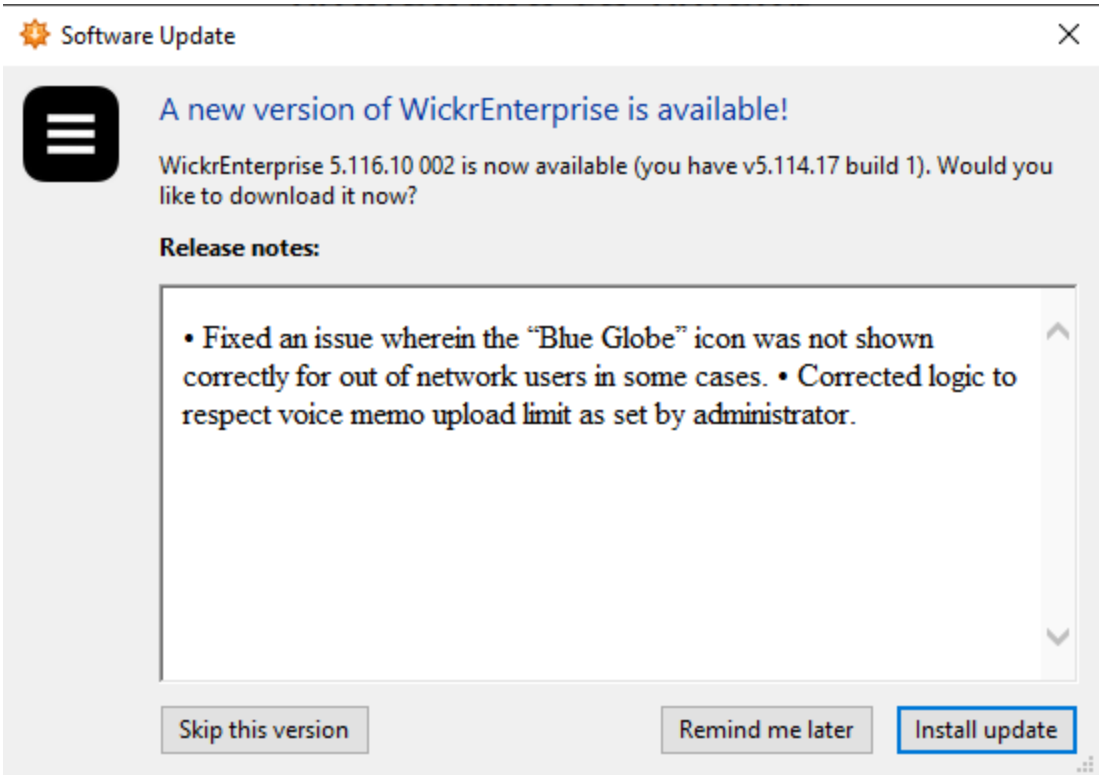


For macOS, Windows, Android and iOS platform versions of the TOE, the user can check for any available software updates using the "Check For Updates" tab on the menu on the left side as shown below. Though the Linux version of the TOE does not provide the "Check For Updates" tab, all other procedures that follow for installing an update are the same for all versions, including the Ubuntu version.

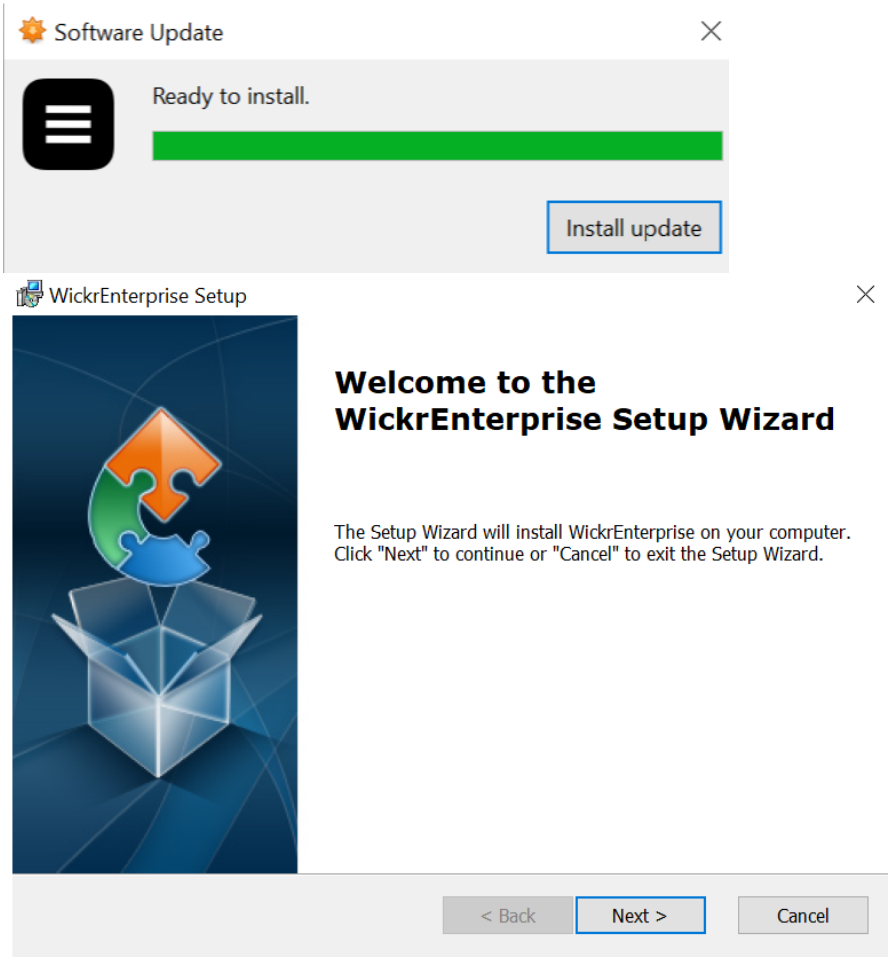


Additionally, a banner pops up across the top of the home screen when an update is available.

When you click “Update”, the current version is displayed as well as the version of the available update along with a prompt to install the update.



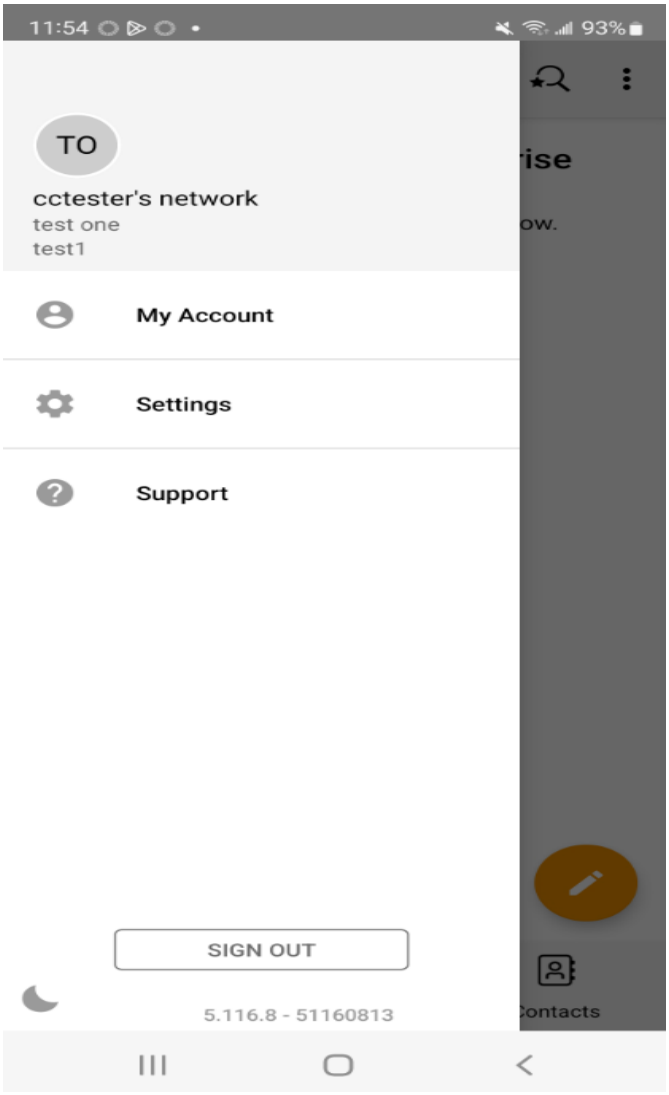
When "Install update" is selected, the updater downloads the update file and then launches the installer, which runs through the same prompts as a fresh installation.



When an installation package is downloaded by the platform, it is verified prior to installation. Updates for the Android and Linux platform versions of the TOE are digitally signed using a 4096-bit RSA key; updates for the iOS, macOS and Windows platform versions of the TOE are digitally signed using a 2048-bit RSA key. Signature verification is performed automatically before proceeding with the package install. If the signature verification fails, the package is not installed.

The administrator can determine whether the update succeeded or failed by checking the TOE's current running version from within the main menu page (as described below), that provides a version number. If the update failed then the version would be the same as before.

The user can view the TOE's current running version that is displayed within the main menu page underneath the sign-out tab at the bottom. This example shows a screenshot for Android and iOS.



Certificate Configuration

Import the certificate needed to validate a TLS server certificate. To install a CA certificate on the device, do the following:

1. Download the certificate.
2. Depending on the platform, perform the following steps:

a. Windows: Double-click the CRT file and click “Install Certificate”. Use the Certificate Import Wizard to import the certificate to either Current User or Local Machine in the Trusted Root Certification Authorities store.

b. Mac: Open the Keychain Access app. Click File > Import Items. Select the CRT file and import to the System keychain. Then right-click the new certificate’s entry in the System keychain. Select “Get Info” and then expand the “Trust” section. Inside this section, select the dropdown next to “When using this certificate: ” and select “Always Trust”.

c. Android: Open the Settings app and navigate to Biometrics and security > Other Security Settings > Install from phone storage. Select the CRT file.

d. iOS: Deploy the CRT file to an accessible web server. Open the Safari app and navigate to the Web server. Select the CRT file and tap “Allow” on the dialog box. Then open the Settings app. A new entry titled “Profile Downloaded” will be present at the top. Tap this item and tap “Install”. Enter passcode if necessary, then tap “Install” one more time. The new root CA should now be present under “Configuration Profiles”. Next, go back to General> tap About> tap Certificate Trust setting. Find the desired Profile (root CA) and click the switch tab to enable the trusted certificate authority.

e. Linux: Copy the CRT file to the directory /usr/local/share/ca-certificates/. Then issue the command “sudo update-ca-certificates”.

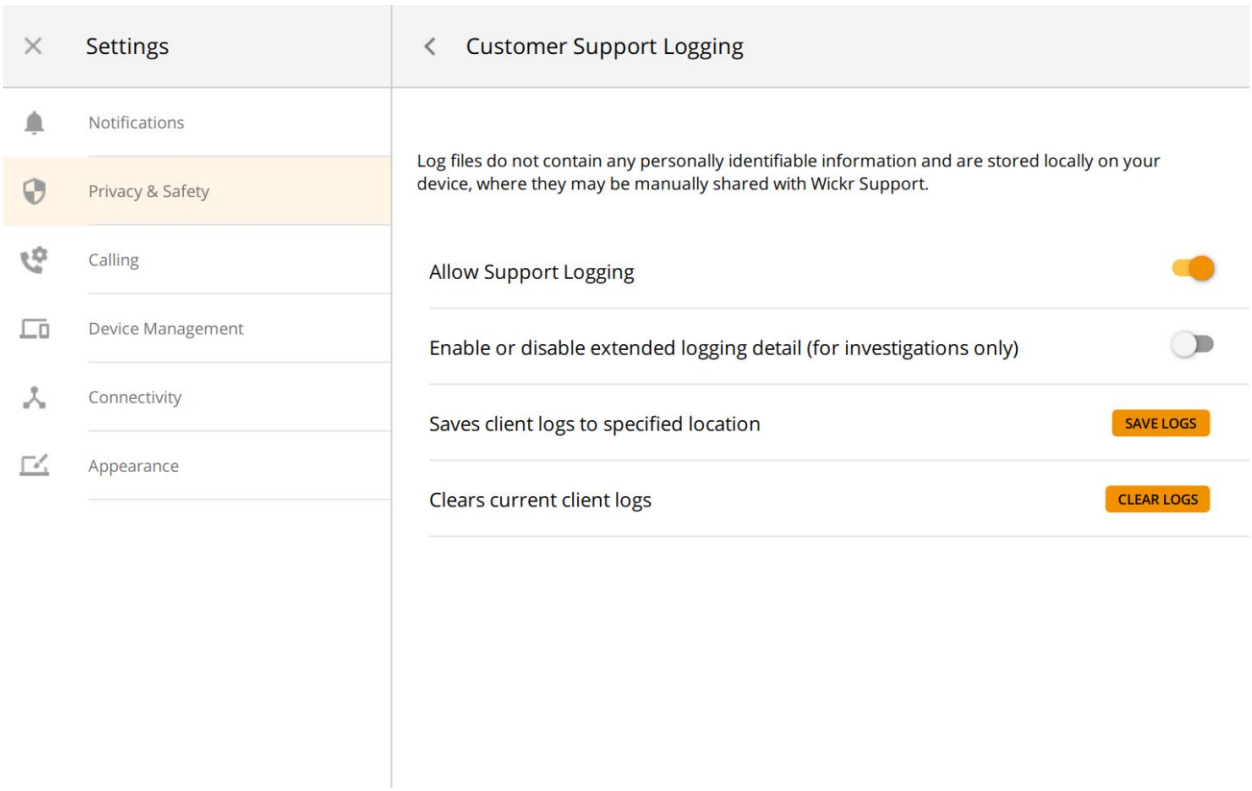
Logging Configuration

Once the application has been installed, the user can enable logging; enable enhanced logging; configure where logs are stored and delete stored logs.

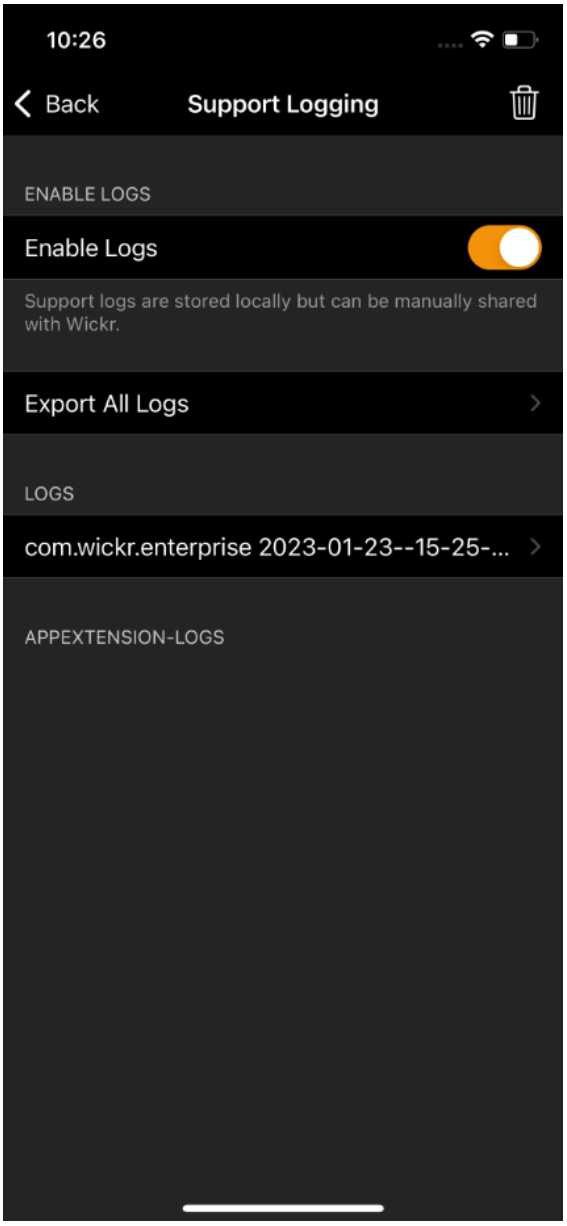
On desktop applications, these settings can be accessed through the menu and then going to Settings > Privacy & Safety > Support Logging, or Support > Support Logging. Both go to the same place.

On mobile applications, you pull open the menu and then go to Support > Support Logging.

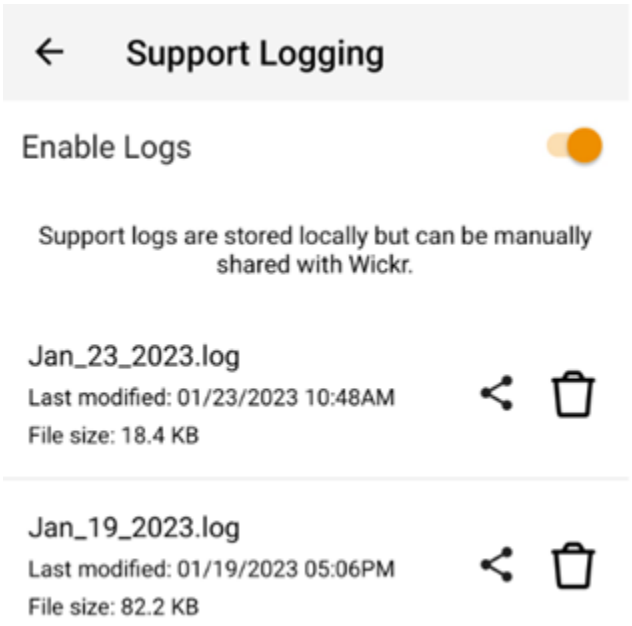
Windows/Mac/Linux:



iOS:



Android:



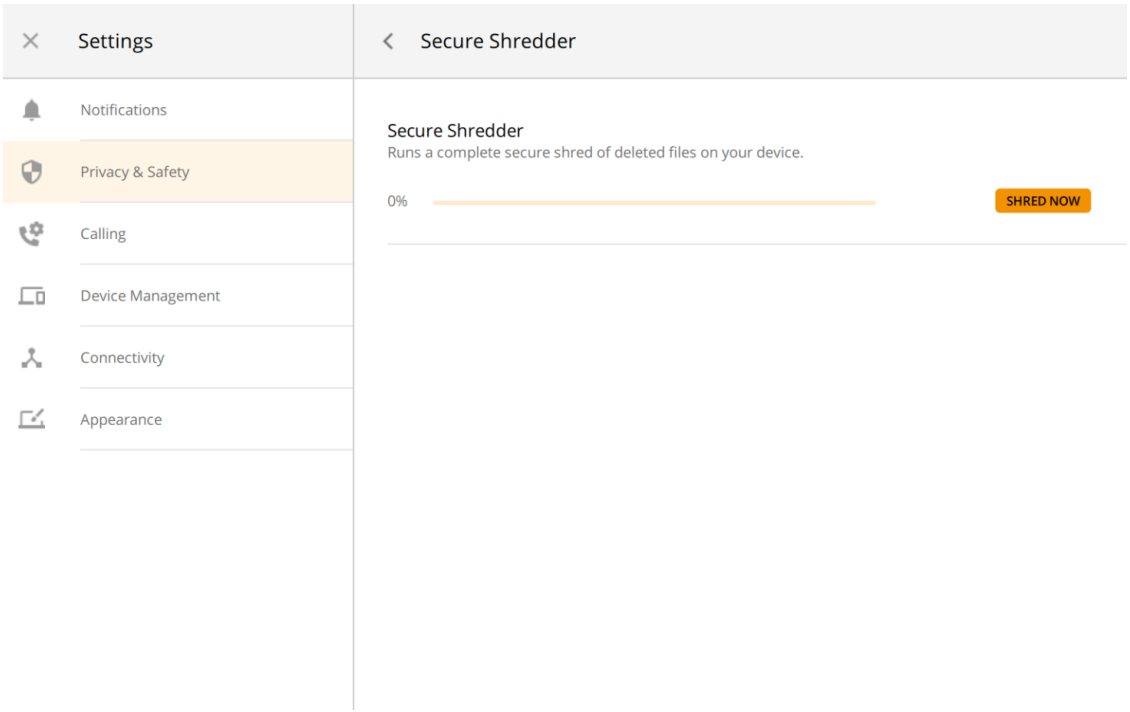
Secure Wipe

The secure wipe shredding function gives users the option to wipe their app data. These settings are also located inside Settings > Privacy & Safety on all platforms.

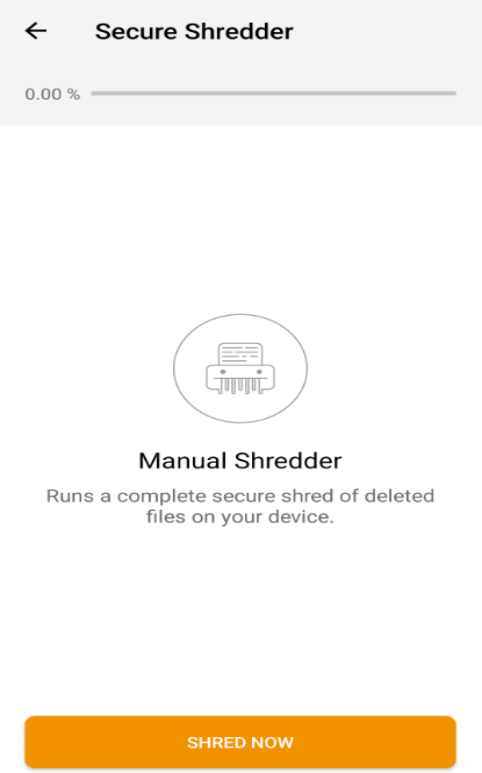
The Wickr shredder will write random data over any RAM and Disk Space used by files opened in the app. This does not apply to files exported, only files opened in a preview within the Wickr apps.

The following are sample screenshots showing the secure wipe shredding options.

Windows/Mac/Linux:



Android:


Secure Shredder
0.00 %
Manual Shredder
Runs a complete secure shred of deleted files on your device.
SHRED NOW

IOS: