CTOUCH®
The power to engage

Security Note

CTOUCH Neo

CONTENTS

Introduction

This document discusses the various security aspects of the CTOUCH displays. This document is organized around the components which make up the CTOUCH Neo product.

Note: this document does not especially touch upon Privacy aspects. Privacy aspects are described in the CTOUCH privacy statement, this document should be seen in conjunction with the CTOUCH privacy statement.

In general

This document describes the security measures that can be taken with the CTOUCH product. Please make yourself aware of the possible security options the product offers. When you order a CTOUCH product in the default setting, we will format all settings in the most user and privacy friendly way possible. Configurating our products is a balance between more secure – less functionality. The customer should always take the setting where the CTOUCH product is used into account when choosing its preferable option. Please also note that a number of add-ons are available for CTOUCH products, which can enhance privacy and security of our products.

Please note that the settings on our products are only part of a security solution. We recommend incorporating the security of the screens into your overall security measures and policies. Pay attention to secure behaviour, like changing pin codes or passwords on a regular basis and not storing pin codes and/or passwords in places that are not safe. Be aware of who uses your screens for what purposes.

Neo: Secure-by-Design

CTOUCH Neo has been designed with security in mind from the start. This means that while we focus on making a very user-friendly touchscreen, we always try to make choices that are secure by default, while not getting in the way of the user. Examples of this are secure default settings, settings default behind a – non-obvious - 6-digit pin code, no user data stored on the screen and automatic browser data removal.

With these settings, we believe that we offer one of the most secure touchscreens on the market, while allowing the administrator to make choices to customise for their organisation.

Secure settings

All Neo settings are default behind a 6-digit pin code. This pin code is set when going through the install wizard and does not allow for obvious pin codes, such as 000000, 012345, 123456. In addition, there is a rate-limiting implemented: When the wrong pin code is entered, it takes a few seconds before you can enter another one.

Neo offers three security levels (Secure, Standard and User friendly) that are set when going through the installation wizard. The most secure level (‘Secure’) does not allow for any data to be stored on the screen itself or on a USB-stick (USB can only be used for touch, video and sound in this mode). In the ‘Standard’ mode, the USB stick can be accessed for touch, video, sound and data, but the screens internal storage is not accessible. The ‘User friendly’ mode gives the greatest amount of freedom, but at the expense of lesser security: It allows for data access to/from both USB storage as well as the screen’s internal storage.

Network and management interfaces – such as ADB and JSON API) are switched off by default and can only be enabled from the pin code protected settings menu.

Applications and data

In order for the Neo to be super user friendly to beginners and advanced users, the Neo screen comes with few applications and tools: CTOUCH Whiteboard, AirServer wireless sharing, (optional) Chromium browser, screenshot tool and annotation tool. These applications have been designed with security and minimal data/network use in mind. The whiteboard, screenshot and annotation tool will not store any data on the screen's storage, on USB or on any server outside the screen. Screenshots are available for the user when the user opens the 'save' button through a dedicated server on the screen itself at a random url for a short amount of time and are deleted after closing the session.

The installation of the Chromium browser is fully optional and decided upon while going through the installation wizard. The Chromium browser has been configured to erase all history, bookmarks, user-accounts, cookies and other possible user data after closing the application or shutting down the screen.

In addition, it is not possible for the user to install any other applications or .apks on the screen, making leaking of data, credentials, histories, etc. very unlikely.

Physical ports

Many of the Neo's physical ports can be enabled and disabled from the - pin code protected - settings menu. This includes all video interfaces (HDMI, DP, USB-C), all USB ports (on/off/touch-only), all network interfaces (all Ethernet ports, Wi-Fi interface, Wi-Fi hotspot and Bluetooth) and the integrated microphone array. In practice, the screen can have exactly the interfaces configured as desired by the screen's manager/admin, even for (semi-)public spaces such as college or university classrooms.

Note that also the other interaction interfaces such as touch, the blue CTOUCH button and remote control interface can be enabled and disabled from the settings menu, making interaction limited to exactly what you want. Lastly, the on-screen buttons in the quick start menu that become available when pushing the CTOUCH button can also be enabled and disabled in the settings menu, making the screen fully configurable and flexible for many applications.

CTOUCH Neo comes with a physical 'Cable lock', a steel protector that can be easily screwed over the connector area of the Neo. This allows for physical protection over the connectors and OPS on the side and bottom of the screen and limits access to these, both from inserting and pulling out. By default this protector is secured by normal Philips screws, but to decrease access even more, security screws can be used.

Network connectivity

As mentioned in the Physical Ports chapter, all network interfaces can be enabled and disabled from the settings menu. The services running on these interfaces are protected by the following means:

- Sphere interface: HTTPS encrypted, security token
- JSON control API: Security token, default disabled

Firmware

CTOUCH is committed to offering a secure touchscreen, now and in the future. This means that we will keep offering firmware updates with bugs fixes, new features and security updates for years to come. In order to make it easy for the user to always have the latest firmware and security fixes, Neo will show a popup when a new firmware is available and allow for direct install. In the settings menu, it is also possible to set the firmware upgrade (typically call Over-The-Air update or OTA update) to fully automatic: In that case, not even a popup will be shown but the latest firmware will be installed automatically the moment it is available.

With our Sphere management system – part of HEARTBEAT service – the IT admin or dealer can check in real-time any of the settings and firmware version and change/update these right from his/her desk. We believe this will make security a breeze for any organisation.

Note: Some new firmware features, bugs fixes and Sphere functionality may only be part of a paid version of HEARTBEAT

More information/questions

In case you would want to know, more details or have questions regarding Neo security: Please contact CTOUCH service (support@ctouch.eu) or your account manager. We are happy to answer your questions and tell you more…